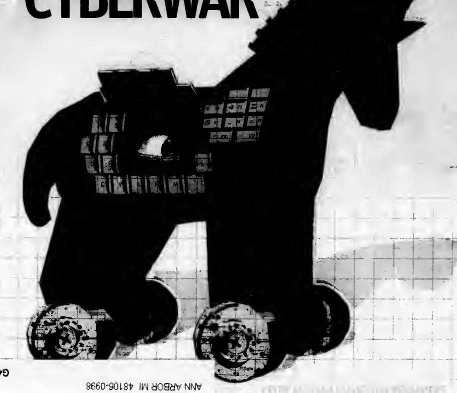
Why Passwords Still Fail Us | Grandpa the Programmer
Windows 8 Faces a Slow Road to the Enterprise

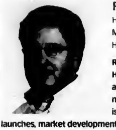
COMPUTERWORLD.

Peer Perspective. IT Leadership. Business Results. | COMPUTERWORLD.COM | NOVEMBER 5, 2012

THE NEW RULES OF CYBERWAR



[illegible] *a rising tide* OF INCREASINGLY SOPHISTICATED AND POTENTIALLY DESTRUCTIVE *attacks* EMANATING FROM HACKTIVISTS, SPIES AND MILITARIZED MALWARE.



Roy Cahn-Speyer
HP PRODUCT MARKETING
MANAGER FOR THE AMERICAS,
HEWLETT-PACKARD CO.

Roy Cahn-Speyer manages HP's BladeSystem enclosure and two-socket server business for the Americas. He is responsible for product launches, market development, and transition planning.

Future-Proof your IT with Smarter Servers

What will the typical two-socket server look like in five years?
The industry is trending toward a server with 64 cores, 4TB to 8TB of memory and two 100Gbit network ports. We think it will be capable of hosting 300 to 500 virtual-machines.

That sounds like a very large server. But what would happen if it were to crash?
Not a pretty picture. That's why at HP, we've started three multiyear projects to address the server of the future. *Project Moonshot* leverages hundreds of low-power processors, like the ones in cell phones, each running its own copy of Linux for applications like Web hosting or Hadoop. *Project Odyssey* aims to improve server reliability and fault tolerance by adapting technology from our NonStop and Business Critical Systems Group to Windows and Linux. And *Project Voyager*, which adds intelligence to our servers, helping to increase uptime, automate server management and reduce the need for staff intervention. In fact, the HP ProLiant Gen8 blade, tower and rack-mount servers, launched in March, are the first deliverables of Project Voyager.

When you're counting on a server farm to power your business, you want a smarter server with intelligence close to the application.

How do these smarter servers powered by AMD Opteron™ 6200 Series processors meet the business needs of CIOs today?
IT managers need to increase server uptime, simplify server management and decrease total cost of ownership. These goals are met by the ProLiant Gen8 servers, which feature a new version of the HP's Integrated Lights-Out processor (iLO 4) iLO 4 delivers a complete set of intelligent, automated management features for self-analysis and healing, from initial deployment to daily management, service alerting and remote support. On the performance and value side, AMD Opteron 6200 Series processors offer the industry's highest core density and the exceptional price/performance that AMD is known for.

Can you explain how iLO 4 delivers a smarter and more automated server?
iLO 4 is like a computer inside each ProLiant Gen8 server. It is connected to all server subsystems and has a 4GB flash memory. iLO 4 enables agentless phone home functionality, which makes remote management painless. HP will even help you manage your servers via our free cloud-based Insight Online portal hosted on hp.com. In addition, the new Active Health System continually monitors and logs 1600 parameters to the 4GB flash memory so even the trickiest problems can be root-caused up to five times faster. We also made initial deployment easier by eliminating the need for CDs. Drivers and firmware needed to install an operating system are now embedded in iLO 4. When it comes time to update firmware and drivers, HP offers the free Smart Update application that automatically sequences every step in the correct order and requires a maximum of one reboot, which takes the risk out of firmware and driver updates.

How is the performance running compute-intensive workloads?
The AMD Opteron 6200 Series processors deliver a major boost in price/performance. Available with 4-, 8-, 12- or 16-core AMD processors, the ProLiant Gen 8 servers feature the highest core density. Twice the cores per server lets you host virtual machines with a dedicated core for each VM. It also lets you serve more database users and solve more complex HPC problems. The Gen8 server design with AMD Opteron 6200 Series processors balances flexibility, expandability and energy efficiency.

What advice would you offer CIOs looking to future-proof their server infrastructure? When you're counting on a server farm to power your business, you want a smarter server with intelligence close to the application. This will enable you to automate manual operations, lower operating costs and increase uptime. Moving in this direction is a journey. We believe the ProLiant Gen8 server with AMD is an excellent place to start.

FOR MORE INFORMATION:
visit www hp com/go/gen8bladeserver2

COMPUTERWORLD
Custom Solutions Group

COMPUTERWORLD

Computerworld.com

EDITORIAL

Editor in Chief

Executive Editor

Managing Editors

Assistant Managing Editor

Director of Blogs

Art Director

Features Editors

News Editors

National Correspondents

Reporters

Editorial Project Manager

Senior Associate Online Editor

Office Manager

Contributing Editors

CONTACTS

Letters to the Editor

News tips

Subscriptions and back issues

Reprints/permissions

THIS ISSUE | 11.05.2012 [VOL. 46, NO. 20 $5/COPY]

FOR BREAKING NEWS, VISIT COMPUTERWORLD.COM

THINKSTOCK / RICHARD BORGE ILLUSTRATION / GETTY IMAGES

HeadsUp

THINKSTOCK

ELECTION WATCH

E-Voting Results: Trust, but Verify

TECHNOLOGY AND process improvements implemented since the controversial 2000 presidential election have made electronic voting machines more secure and reliable, according to a recent report by the Caltech-MIT Voting Technology Project.

Even so, the only way to absolutely ensure the integrity of e-votes cast is to audit the results and all voting technologies used in an election, the 85-page report cautioned.

Rather than setting security standards for voting equipment, the best way to ensure ballot integrity is to hand-count a large and random sample of the paper records of votes cast electronically, the report said.

The Voting Technology Project was launched to investigate the causes of the voting problems in Florida in 2000 and to make recommendations based on its findings.

Some progress has been made since 2000, said Michael Alvarez, co-director of the Voting Technology Project. The antiquated, lever-activated punch-card voting systems that led to the infamous hanging-chad fiasco in Florida have been mostly replaced with more reliable optical-scan and electronic voting systems, he said. This year, only a small number of voting districts will use purely hand-counted paper ballots; most will use some form of electronic system that has a way of verifying e-votes with a paper record.

However, Alvarez said, few jurisdictions have further upgraded voting equipment in recent years. He said he hopes to see that situation "change as public finances improve."

– Jaikumar Vijayan

SECURITY

Sharing Systems Could Help Firms Survive Hacks

Groups of companies in the same industry could mitigate the effects of cyberattacks by pooling infrastructure resources and working together on security issues, a senior official in the U.S. Department of Homeland Security has suggested.

The comments by Mark Weatherford, deputy undersecretary for cybersecurity, came as several U.S. banks were dealing with a fourth week of distributed denial-of-service (DDoS) attacks.

The targeted banks include Wells Fargo, U.S. Bancorp, PNC Financial Services Group, Citigroup, Bank of America and JPMorgan Chase. Hackers in Iran have claimed responsibility.

"This has been an eye-opening experience," said Weatherford, speaking at a cybersecurity awareness conference in Santa Clara, Calif., organized by local businesses.

Weatherford suggested "a co-op kind of model" where Internet service providers buy many more servers than any one company might need and then "co-op that for like-minded organizations" so that when someone needs the capacity, it would be available.

"We need to think of different ways of sharing resources," he said, but also acknowledged that he has "no idea" if such a scheme is legal or even possible.

– MARTYN WILLIAMS, IDG NEWS SERVICE

COMPUTERWORLD.COM

BETWEEN THE LINES

By John Klossner

IT CAREERS

Gartner Upbeat on Big Data Jobs

THE ECONOMIC PICTURE that Gartner's head of research, Peter Sondergaard, painted at his firm's recent Symposium/ITxpo conference in Orlando was upbeat in a surprising way.

While Gartner isn't significantly raising its global IT growth forecast — which it revised downward earlier in the year — its relatively flat forecast doesn't apply to at least one sector of IT: the big data labor market.

Big data, which refers to the vast amounts of information collected from every imaginable source, is becoming an engine of job creation as businesses strive to harness and analyze that data in order to glean revenue-generating insights from it, according to Gartner.

Between now and 2015, the firm expects big data to create some 4.4 million IT jobs globally; of those, 1.9 million will be in the U.S. Applying an economic multiplier to that estimate, Gartner expects each new big-data-related IT job to create work for three more people outside the tech industry, for a total of almost 6 million more U.S. jobs.

But Sondergaard's estimate included this caveat: There's a serious shortage of IT professionals with big-data skills, and only one-third of those new jobs will be filled.

"There's not enough talent in the industry," he said, adding that education "is failing us."

Griff Law, CTO of Northeast Georgia Health System, agreed that it's difficult to fill data analytics positions — and IT jobs in general. He said his company has had 15 open IT positions for six months.

About six of those openings are either for business analysts with business intelligence and analytics skills or clinical analysts with both IT and data skills. The company's other IT job openings include positions for network engineers.

Overall, Gartner expects IT spending to rise to $3.7 trillion worldwide next year, a 3.8% increase over this year.

– Patrick Thibodeau

Micro Burst

Citing a slump in the PC market, AMD says it will lay off

1,800

EMPLOYEES,

or 14% of its workforce.

DATA CENTER

GM Plans to Hire 3,000 HP IT Workers

Hewlett-Packard has agreed to transfer 3,000 of its employees to General Motors, as the automaker moves IT operations in-house, the two companies announced.

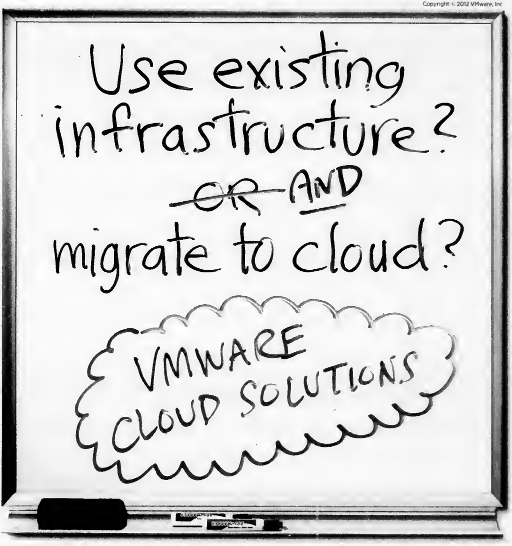
The HP workers are part of a team running GM's IT operations under outsourcing contracts. GM CIO Randy Mott said the car company hopes to add them to its payroll over the next six months.

Mott, named CIO of GM earlier this year, decided early in his tenure to bring most of the automaker's IT work in-house, a major shift for a company that has long relied on outsourcers. Under Mott, GM is consolidating and automating IT operations, and plans to put the savings toward innovation of its product lines and business operations.

GM plans to reduce its worldwide roster of data centers from 23 to two within three years. It also wants to cut the number of applications it uses by 40%, according to Mott.

HP will continue to have a role in GM's IT operations. The agreement between the two companies calls for GM to use HP's IT Performance Suite and Enterprise Security Suite, as well as data analytics and business intelligence software in the vendor's Vertica and Autonomy product lines.

– PATRICK THIBODEAU


Use existing
infrastructure?
~~OR~~ AND
migrate to cloud?
VMWARE
CLOUD SOLUTIONS

Windows 8 Faces A Slow Road to The Enterprise

As Microsoft's next-generation operating system finally makes its debut, it faces a high-stakes battle with iOS and Android.

By Patrick Thibodeau and Joab Jackson

NOW THAT Microsoft has finally launched its next-generation operating system, Windows 8, it must tackle what may be the most daunting marketing challenge it has ever faced.

Once the supreme leader of personal computing, Microsoft is now just one of several competitors in a brave new world in which PCs are losing ground to tablets and smartphones — platforms on which Windows has a minor presence.

At the Windows 8 launch event in New York late last month, Microsoft CEO Steve Ballmer called Windows 8 a radical change from previous versions of the company's flagship operating system. Windows, he said, has been recast to provide a unified interface across a range of devices, from smartphones to tablets to traditional PCs.

Microsoft officials acknowledge that much has changed in the three years since the last major Windows release, Windows 7. "In Windows 8, we shunned the incremental," said Steven Sinofsky, president of the Windows and Windows Live division.

Thanks to Moore's Law and dramatic improvements in technology, it's now possible to give users access to a good deal of computing power via handheld devices, creating opportunities for alternative operating systems like Apple's iOS and Google's Linux-based Android.

Nonetheless, Sinofsky contends that Windows 8 can build on the success of predecessors like Windows 7, which he called "the most successful operating system ever released," noting that 670 million Windows 7 licenses have been sold.

Any early success will have to come from consumers, because enterprises aren't likely to quickly adopt Windows 8, according to research firm Gartner.

"There are no compelling business imperatives to drive legacy devices in business toward Windows 8," said Gartner analyst Peter Sondergaard at his firm's annual Symposium/ITexpo conference last month. He predicted that any widespread corporate move to Windows 8 won't happen until "at least 2014."

Gartner said its projection doesn't mean Windows 8 is already on the ropes. Large enterprises rarely move quickly to new Microsoft operating systems. Applications have to be tested, and many IT shops wait for the release of the first service pack.

Gartner analysts expect to see selective rollouts of Windows 8. The emergence of tablets and smartphones as the primary tools for some enterprise workers, such as salespeople, means the days of massive, enterprisewide upgrades of a single standard platform are over.

Derek Minnich, an IT program manager at a company that he asked not be named, said his employer has used Windows 7 for about two years and there's no reason to upgrade at this point.

The only thing that might speed a move to Windows 8 would be "if tablets overtake the PC rapidly," Minnich said. Users will want Office products on tablets, and "that's where the [Windows 8] entry point will be," he said.

Peter Nies, who works in information security at a company that he asked not be named, said a significant amount of user training may be required to help familiarize people with the dramatic new features in Windows 8, such as its tiles and new interface.

"From a user perspective, it scares me because it is so radically different," said Nies. ◆

***Jackson** is a reporter for the IDG News Service. **Juan Carlos Perez** of the IDG News Service and **Gregg Keizer** contributed to this story.*

There's no compelling business imperatives to drive legacy devices in business toward Windows 8."

MICROSOFT

MIDSIZE BUSINESSES ARE THE ENGINES OF A SMARTER PLANET

FROM LIMITED I.T. RESOURCES TO UNLIMITED POTENTIAL.

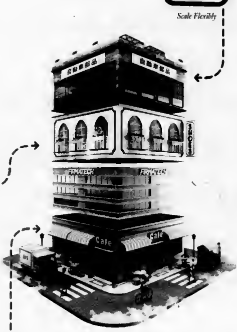
FOR MIDSIZE BUSINESSES, A REDEFINING MOMENT.

In the past, midsize organizations with big ideas were constrained by limited IT resources. Not anymore. With the arrival of scalable, affordable cloud computing, sophisticated ideas for new products no longer languish. Personalized customer service generates incremental sales. And new, revenue-rich markets are being created every day.

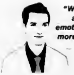
It's shaking up industries and providing new opportunities for new players, with many pioneering midsize businesses once again leading the way. Consider: 92% of midsize companies say they will pilot or adopt a cloud solution within the next 36 months.

Progressive companies like LINK Institute, the Swiss consumer research firm with 110 employees, are doing it right now.

92% *92% of midsize companies say they will invest in the cloud within the next 36 months.**



What can the cloud do for your midsize business?



"We can assess a consumer's emotive response more accurately."
– Tim Llewellynn, nViso CEO

REINVENT WITHOUT REINVESTING IN I.T.

LINK wanted a faster, more accurate way to measure consumer sentiment. Working with a powerful facial recognition solution created by IBM Business Partner nViso in the IBM SmartCloud,™ LINK is now capturing respondent reactions to marketing messages in real time, via home webcams. Scores are generated every second for 7 emotions. And LINK gets its results up to 90% faster.

In the past, a data-rich solution like LINK's would have been impractical for a midsize company. But in the cloud, traditional research is history. And a new service has transformed a business.

Get started by learning how IBM and its Business Partners are helping midsize businesses reinvent themselves at **ibm.com/engines/cloud**

LET'S BUILD A SMARTER PLANET.

IBM.

*2011 IBM Institute for Business Value/Economist Intelligence Unit Cloud-Enabled Business Model Survey. IBM, the IBM logo, ibm.com, IBM SmartCloud, Smarter Planet and the planet icon are trademarks of International Business Machines Corp., registered in many jurisdictions worldwide. A current list of IBM trademarks is available on the Web at www.ibm.com/legal/copytrade.shtml.

DreamWorks relies on state-of-the-art IT to produce animated features like *Madagascar 3*.

Inside the DreamWorks Data Center

The movie studio invests heavily in IT to keep its animation artists efficient – and happy.

By Lucas Mearian

CONVENTIONAL WISDOM would likely conclude that a creative, IT-driven company like DreamWorks Imagination Studios must embrace all of the latest computing trends and that cutting-edge technologies like the cloud, virtualization and solid-state storage play leading roles in its data center.

Conventional wisdom would be mostly wrong.

About 15% of the servers at DreamWorks are virtualized, about 20% of the movie maker's computer-generated image rendering is performed using cloud services, and the company has yet to find a need for solid-state drives, said Mike Cutler, global director of infrastructure operations.

The studio does, however, invest heavily in state-of-the-art server blades, storage arrays and networks to make sure its animation artists have the tools they need, Cutler said during a recent tour of the company's studio and data center in Redwood City, Calif.

The data center features about 3.8 petabytes of disk storage capacity and 4,000 servers with 25,000 CPU cores.

DreamWorks, which has two studios in the U.S. and one in India, tries to release three animated movies a year. One film takes about three years to create, so the company is usually working on eight to 10 productions at any one time.

The studio must invest in IT "to make sure our artists and engineers stay happy," said Kate Swanborg, head of enterprise marketing. "If we don't stay a couple steps ahead of state-of-the-art, they'll try to find it somewhere else."

The processing power and storage capacity required to produce computer-generated 3D films can be tremendous — DreamWorks uses more than 300 high-end workstations.

The studio's servers run some 400,000 processing jobs per day and use Red Hat's Enterprise MRG integrated high-performance computing platform to schedule those jobs. "Most of it is done in parallel," Cutler said.

Not including developers working directly on film productions, DreamWorks has 150 software engineers who write applications and keep them and third-party products running smoothly, said Jeff Wike, director of R&D at the Redwood City studio. About 20% of the company's software engineers have Ph.D.s, he added.

For the past three years, the software engineers have been "parallelizing [in-house] software" to take advantage of the latest Intel 16-core Sandy Bridge processors in its servers, Wike said.

"We don't write all of our software, but we do write a lot of it. We buy where we can and build where we must," he said.

The cost of producing a DreamWorks film can be staggering: as much as $130 million for one 90-minute feature film, such as *Shrek 4*.

DreamWorks has standardized much of its IT infrastructure on Hewlett-Packard BladeSystem c-Class server blades; 3,000 of those are part of a preconfigured computing, storage and network architecture. It also uses HP NAS and 3Par storage arrays, along with a few Hitachi Data Systems and NetApp drives.

The pending release of MGM's film adaptation of *The Hobbit* could raise the IT stakes for all animation studios: It will be the first motion picture made using 48-frames-per-second technology. "If that's an experience consumers appreciate, it will have a huge impact on storage and rendering [needs]," Wike said.

Of course, investing in new technology to meet a new production standard always carries a price tag. "But if it provides a premium experience people are willing to pay for, that's OK," said Swanborg. "That's a great trade-off." ◆

"We buy [software] where we can and build where we must."

DREAMWORKS

NO POSTAGE
NECESSARY
IF MAILED
IN THE
UNITED STATES

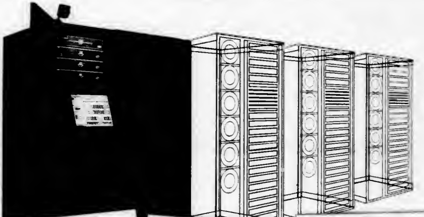
BUSINESS REPLY MAIL
FIRST-CLASS MAIL PERMIT NO. 36 WEST KINGSTON, RI

POSTAGE WILL BE PAID BY ADDRESSEE

APC
by Schneider Electric

ATTENTION CRC: v473v
APC BY SCHNEIDER ELECTRIC
132 FAIRGROUNDS ROAD
WEST KINGSTON RI 02892-9901

Only our IT physical infrastructure is as dynamic as your business needs.



"The ability to monitor everything from the Web allows us to catch small problems before they become a big concern."

Andy Koostra
Systems Manager
Consolidated Utility District

"This solution ensures a single integrated power and cooling management system."

Brian R. York – Director
Wireless National Practice
Insight

"APC by Schneider Electric InRow™ cooling architecture... is our design standard going forward."

Mike Mallett – Director of technical operations
Saint Luke's Health System

Protect any IT equipment or deployment with our adaptable APC by Schneider Electric InfraStruxure solutions.

A solution for every IT configuration

Protect your IT system uptime easily where ever your IT is deployed with APC InfraStruxure™ solutions. Our simple, adaptable, and manageable all-in-one physical infrastructure is designed as an easy-to-deploy system to allow for flexible management, physical IT deployment, and by extension, system uptime.

Customers have adapted the solution to all IT configurations — from out-of-the-way network closets to server rooms to data centers. Power protection, cooling, rack systems, and remote management are part of the total architecture for highest availability at all times. With our InfraStruxure solutions working to stave off physical threats, you can focus on more pressing concerns such as network threats, IT hardware failure, and switch hang-ups. When you deploy our solution, it's as if you're getting another IT person to ensure that your IT space or data center will still be at your command when you need it. What's more, our life cycle services enable optimal operations.

InfraStruxure

Integrated InfraStruxure solutions include everything for your IT physical infrastructure deployment: backup power and power distribution, cooling, enclosures, and management software. Adaptable solutions scale from the smallest IT spaces up to multi-megawatt data centers.

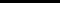
Mission-critical IT infrastructure without the complexity

> Simple
Solution guides and out-of-the-box installation make deployment easy

> Manageable
Remote monitoring, management, and reporting simplify IT operations; energy management cuts costs.

> Adaptable
With standardized designs for all types of applications, our solutions can be adapted to fit any IT need at any time for business-minded flexibility.

Business-wise, Future-driven.™



Make the most of your IT space!

Download our Top 3 solution design guides today and enter to win an iPad® 2.

Visit: www.apc.com/promo Key Code: v473v Call: 888-289-APCC x6475

APC™
by Schneider Electric

THE Grill

Christopher Perretta

With technology as the driver, this CIO maps a financial giant's strategy.

What's the most effective approach to time management? "Don't sweat the small stuff."

What's your favorite way to spend downtime? "[I have a] growing affinity for power tools."

Where is your hometown? Westbury, N.Y.

Is there anything that very few people know about you? "I'm an ex-medical engineer."

What are you reading now? *Arguably: Essays by Christopher Hitchens*

PHOTO COURTESY OF STATE STREET

STATE STREET'S *executive vice president and CIO, Christopher Perretto, says technology is leoding the transformation of the finoncial services industry. In any arganizotion ot ony time, that's na small tosk, but Perretto says it's porticularly chollenging given the stote of the economy in the past several yeors. But he welcomes the opportunity. "I aspire to be o change agent," says Perretto, who leods a team of more thon 5,000 employees and contractors thot supports operations in 27 countries. His leadership was recognized eorlier this yeor, when he received on MIT Sloan CIO Symposium 2012 Award for Innovation Leodership. The oward honors CIOs who leod their orgonizations to pursue the innovative use of IT ond business procésses to deliver business value.*

What do you think earned you the MIT distinction? I think the team at State Street has done a great job at really putting new technology into a business context, and they're making a difference with the business. They're a very customer-centric group and a

SSD 840 PRO.
Performance at a different level.
SAMSUNG
[illegible] State D[illegible]
[illegible]
www samsung com/ssd
SAMSUNG

KENT [illegible]

> **Everything we do from a development standpoint has to have a commercial return. It's as straightforward as that.**

tech-savvy group, and they've made the connection between those two ideas. They've delivered in an environment that requires some pretty high-quality delivery. I'm proud to be a part of that team.

What's your role in all that? My job is to connect the dots, to build an organization that leverages the talent that we have. I think at State Street we've elevated the role of architecture, of technology architect — and I use that word to include application architect, data architect, technical architect. We've elevated that role and made it a firm-wide endeavor, and that has greatly enhanced our ability to deliver solutions in a consistent manner across the board.

What are the most important qualities in an IT leader today? It's very easy to get into the tech tactical side of what we do and the incident management side of what we do, and one has to fight to free up the resources and the brain space to develop strategies and execute on them. You get sucked into the day-to-day, and you have to make an effort to build capabilities that are geared for five years from now. You can't lose the day-to-day, but you can't forgo the strategy. And then you have to execute on the strategy. So you have to build the organization and work with the people. [You have to determine:] Are you putting the right people in the right spot and giving them the right type of autonomy to do their jobs?

How would you summarize your vision for IT at State Street? In financial services, technology plays an expansive role. It is the physical manifestation of the product. We're both engineering and manufacturing and maintaining [the product], and we actually drive the car. And as technology grows — and with Moore's Law, where processing power doubles every 18 months — technology's role will grow in financial services. Technology is at the heart of what we need to accomplish from an operational standpoint. Technology has to grow with the business, and it has to be a key driver of business rather than just being an enabler.

How do you, as CIO, craft a strategic position and ensure that colleagues and staff are on board with that position? We start with the business strategy. We say, "What are the imperatives that we have, what capabilities does the organization need, and what are the attributes the organization has to have in the current environment and to fulfill the strategic plan?" And we put our investments and efforts in that context. Everything we do from a development standpoint has to have a commercial return. It's an investment in time and money, and we need to get a return. And that return has to be consistent with where we want the business to go. It's as straightforward as that. When you can connect major technology initiatives to the strategy of tbe firm in quantifiable ways, you can present to senior management a proposition that's appealing.

How do you encourage innovation in your organization? We kind of look at it as a pipeline. We have a couple of groups that are part of that pipeline. We have a chief scientist, and his job is to say, "What are the technologies out there that are likely to be impactful to our business, what are tbe potential uses of social media, or when should we be looking at certain hardware technologies?" Then we have the architecture group, which is really chartered with piloting new technologies and new approaches in real-world environments to demonstrate utility to the approach or technology. And when they're successful, we industrialize it for use by tbe whole organization. I always tell my head of architecture he has to be three or four years out for me, because those are the kind of horizons the business uses.

How does a CIO create a cohesive team in such a large operation? We don't think about it as passing work around the globe. It's not like, "Send this work over to China to get done or down to New Jersey." Instead, we think, "We have a team made up of people from around the world." And when you do that, it's a lot easier because they're working together. We also benefit from the [fact] that 75% of the work we do is for global consumption, so they're consistently considering the implication to all, not just for North America. That helps teams stay together. I think State Street has a strong culture in its own right, too, that's about global inclusion and serving those customers. And our customers are more global than ever before.

— Interview by Computerworld *contributing writer* **Mary K. Pratt** *(marykpratt@verizon.net)*

data for :
the brave
DMAT

OPINION

S.J. VAUGHAN-NICHOLS

Grandpa the Programmer

Too many of us of a 'certain age' are facing an IT work environment that's hostile to older workers.

I'M 56. I'm not a grandfather — not yet anyway — but I'm old enough to be one. I first used the Internet in the '70s. My first programming language was IBM 360 Assembler. My first operating system was the IBM mainframe's OS/360. I was the first journalist to write about this new network service called the Web and say it just might matter.

You know what? I think I may just know a wee bit about computing.

I'm far from the only one. Lately, though, I've been noticing that the old meme about how grandpa can't understand iPhones, Linux or the cloud seems to be showing up more often even as it's becoming increasingly irrelevant. I've been guilty of using it myself.

Think about it. The big names of our field? Dennis Ritchie, creator of C and Unix, was 70 when he died last year. Ken Thompson, co-creator of Unix, is 67. James Gosling, founder of Java, is 57. Bill Gates is 56. So is Steve Ballmer. Steve Jobs was 56 when he left us. Tim Cook, his successor as head of Apple, is 51.

Linux and open source? Free software founder Richard M. Stallman is 59. His open-source philosophical rival Eric S. Raymond is 54. And even Linus Torvalds is now on the "older" side of 40, at 42.

And it's not just the big names: 27% of social network users are 45 or older.

We baby boomers like to think of ourselves as forever young. We're not. Some of us are now well into retirement. Too many of us of a "certain age" are facing an IT work environment that's hostile to older workers.

I wonder if perhaps that's why I've been hearing more about how "older" people don't get technology. Maybe that's meant to hide the age bias that is the IT business's dirty little secret.

True, people in their 50s who have families are less likely to have any desire to work 80-plus-hour weeks, but so what? Frederick Brook's *The Mythical Man-Month*, a classic of software management, blew out the delusion decades ago that simply throwing more man-hours at an IT problem fixes anything.

Experience Counts

Sadly, while that should have put an end to the idea that long hours are a fact of IT life, this remnant of our factory-line past lingers both in high tech and in other industries. But what really matters is who's productive and who's not.

In some jobs, such as law and accounting, the billable hour is all. The system encourages people to burn as many hours as possible on any given task. That's not how it is in IT, though. We need to get work done as fast as possible with as few mistakes as possible.

Guess what? Experienced grandpas or grandmas who cut their teeth on C can be just as effective as any 20-year-old wunderkind who's a wiz at JavaScript.

That's not to say that older workers are always better. I've known far too many people who "retire in place." They don't bother learning new skills. They can't understand that the same old server thinking doesn't work in an era in which everyone is migrating to the cloud.

But — and this is the important thing — good older IT workers can deliver just as much, if not more, than their younger counterparts. Remember, grandpa not only understands technology, he may well have helped invent it. ◆

Steven J. Vaughan-Nichols has been writing about technology and the business of technology since CP/M-80 was cutting-edge and 300bps was a fast Internet connection — and we liked it! He can be reached at sjvn@vna1.com.

THE NEW RULES *of* CYBERWAR

CRITICAL INFRASTRUCTURE PROVIDERS FACE A ALMOST *a rising tide* OF INCREASINGLY SOPHISTICATED AND POTENTIALLY DESTRUCTIVE *attacks* EMANATING FROM HACKTIVISTS, SPIES AND MILITARIZED MALWARE.

BY ROBERT L. MITCHELL

THREE YEARS AGO, when electric grid operators were starting to talk about the need to protect critical infrastructure from cyberattacks, few utilities had even hired a chief information security officer.

Then came Stuxnet.

In 2010, that malware, widely reported to have been created by the U.S. and Israel, reportedly destroyed 1,000 centrifuges that Iran was using to enrich uranium after taking over the computerized systems that operated the centrifuges.

RICHARD BORGE ILLUSTRATION

Gen. Michael Hayden, principal at security consultancy The Chertoff Group, was director of the National Security Agency, and then the CIA, during the years leading up to the event. "I have to be careful about this," he says, "but in a time of peace, someone deployed a cyberweapon to destroy what another nation would describe as its critical infrastructure." In taking this step, the perpetrator not only demonstrated that control systems are vulnerable, but also legitimized this kind of activity by a nation-state, he says.

The attack rattled the industry.

Mark Weatherford

Stuxnet was a game-changer because it opened people's eyes to the fact that a cyber event can actually result in physical damage," says Mark Weatherford, deputy undersecretary for cybersecurity in the National Protection Programs Directorate at the U.S. Department of Homeland Security.

In another development that raised awareness of the threat of cyberwar, the U.S. government in October accused Iran of launching distributed denial-of-service (DDoS) attacks against U.S. financial institutions (see related story, page 4). In a speech intended to build support for stalled legislation known as the Cybersecurity Act that would enable greater information sharing and improved cybersecurity standards, Defense Secretary Leon Panetta warned that the nation faced the possibility of a "cyber Pearl Harbor" unless action was taken to better protect critical infrastructure.

"Awareness of the problem has been the biggest change" since the release of Stuxnet, says Tim Roxey, chief cybersecurity officer for the North American Electric Reliability Corp. (NERC), a trade group serving electrical grid operators. He noted that job titles such as CISO and cybersecurity officer are much more common than they once were, new cybersecurity standards are now under development, and there's a greater emphasis on information sharing, both within the industry and with the DHS through sector-specific Information Sharing and Analysis Centers.

On the other hand, cybersecurity is still not among the top five reliability concerns for most utilities, according to John Pescatore, an analyst at Gartner. Says Roxey: "It's clearly in the top 10." But then, so is vegetation management.

Compounding the challenge is the fact that regulated utilities tend to have tight budgets. That's a big problem, says Paul Kurtz, managing director of international practice at security engineering company CyberPoint International and former senior director for critical infrastructure protection at the White House's Homeland Security Council. "We're not offering cost-effective, measurable solutions," he says. "How do you do this without hemorrhaging cash?"

Falling Behind

Most experts agree that critical infrastructure providers have a long way to go. Melissa Hathaway, president of Hathaway Global Strategies, was the Obama administration's acting senior director for cyberspace in 2009. That year, she issued a Cyberspace Policy Review report that included recommendations for better protecting critical infrastructure, but there hasn't been much movement toward implementing those recommendations, she says. A draft National Cyber Incident Response plan has been published, but a national-level exercise, conducted in June, showed that the plan was insufficient to protect critical infrastructure.

"A lot of critical infrastructure is not even protected from basic hacking. I don't think the industry has done enough to address the risk, and they're looking for the government to somehow offset their costs," Hathaway says. There is, however, a broad recognition that critical infrastructure is vulnerable and that something needs to be done about it.

The Department of Defense has a direct stake in the security of the country's critical infrastructure because the military depends on it. "The Defense Science Board Task Force did a review of DOD reliance on critical infrastructure and found that an astute opponent could attack and harm the DOD's capabilities," says James Lewis, a senior fellow specializing in cybersecurity at the Center for Strategic and International Studies.

At a forum in July, NSA Director Gen. Keith Alexander was

RISE OF THE STATE-SPONSORED ATTACKER

JANUARY 2010
Operation Aurora

A [illegible] attack that [illegible] a ware [illegible] atched [illegible] Explorer

- **Purpose:** [illegible] information [illegible] companies [illegible] Google [illegible]
- **Suspected author:** [illegible]

JUNE 2010
Stuxnet

The first malware weapon [illegible]ed to physically destroy critical infrastructure

- **Purpose:** To take over control systems and destroy [illegible] centrifuges used to purify uranium by forcing them to spin out of control
- **Suspected authors:** [illegible] the United States

SEPTEMBER 2011
Duqu

A Trojan malware

- **Purpose:** Espionage

Duqu was designed to provide a back door for stealing information from infected computers

- **Suspected authors:** Israel and the United States

MAY 2012
Flame

A worm that records [illegible] screenshots, keyboard [illegible] and network traffic [illegible] Windows computers

- **Purpose:** Cyber espionage against countries in the Middle East
- **Suspected authors:** Israel and the United States

Gen. Michael Hayden, principal at security consultancy The Chertoff Group, was director of the National Security Agency, and then the CIA, during the years leading up to the event. "I have to be careful about this," he says, "but in a time of peace, someone deployed a cyberweapon to destroy what another nation would describe as its critical infrastructure." In taking this step, the perpetrator not only demonstrated that control systems are vulnerable, but also legitimized this kind of activity by a nation-state, he says.

Mark Weatherford

The attack rattled the industry. "Stuxnet was a game-changer because it opened people's eyes to the fact that a cyber event can actually result in physical damage," says Mark Weatherford, deputy undersecretary for cybersecurity in the National Protection Programs Directorate at the U.S. Department of Homeland Security.

In another development that raised awareness of the threat of cyberwar, the U.S. government in October accused Iran of launching distributed denial-of-service (DDoS) attacks against U.S. financial institutions (see related story, page 4). In a speech intended to build support for stalled legislation known as the Cybersecurity Act that would enable greater information sharing and improved cybersecurity standards, Defense Secretary Leon Panetta warned that the nation faced the possibility of a "cyber Pearl Harbor" unless action was taken to better protect critical infrastructure.

"Awareness of the problem has been the biggest change" since the release of Stuxnet, says Tim Roxey, chief cybersecurity officer for the North American Electric Reliability Corp. (NERC), a trade group serving electrical grid operators. He noted that job titles such as CISO and cybersecurity officer are much more common than they once were, new cybersecurity standards are now under development, and there's a greater emphasis on information sharing, both within the industry and with the DHS through sector-specific Information Sharing and Analysis Centers.

On the other hand, cybersecurity is still not among the top five reliability concerns for most utilities, according to John Pescatore, an analyst at Gartner. Says Roxey: "It's clearly in the top 10." But then, so is vegetation management.

Compounding the challenge is the fact that regulated utilities tend to have tight budgets. That's a big problem, says Paul Kurtz, managing director of international practice at security engineering company CyberPoint International and former senior director for critical infrastructure protection at the White House's Homeland Security Council. "We're not offering cost-effective, measurable solutions," he says. "How do you do this without hemorrhaging cash?"

Falling Behind

Most experts agree that critical infrastructure providers have a long way to go. Melissa Hathaway, president of Hathaway Global Strategies, was the Obama administration's acting senior director for cyberspace in 2009. That year, she issued a Cyberspace Policy Review report that included recommendations for better protecting critical infrastructure, but there hasn't been much movement toward implementing those recommendations, she says. A draft National Cyber Incident Response plan has been published, but a national-level exercise, conducted in June, showed that the plan was insufficient to protect critical infrastructure.

"A lot of critical infrastructure is not even protected from basic hacking. I don't think the industry has done enough to address the risk, and they're looking for the government to somehow offset their costs," Hathaway says. There is, however, a hroad recognition that critical infrastructure is vulnerahle and that something needs to be done about it.

The Department of Defense has a direct stake in the security of the country's critical infrastructure because the military depends on it. "The Defense Science Board Task Force did a review of DOD reliance on critical infrastructure and found that an astute opponent could attack and harm the DOD's capabilities," says James Lewis, a senior fellow specializing in cybersecurity at the Center for Strategic and International Studies.

At a forum in July, NSA Director Gen. Keith Alexander was

RISE OF THE STATE-SPONSORED ATTACKER

Purpose

Suspected authors

Purpose

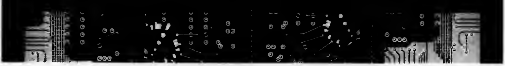
Suspected authors

Purpose

Suspected authors

Purpose

Suspected authors



THINKSTOCK

1&1 DEDICATED SERVERS

SAVE $480

Our data centers offer top security, Cisco firewall protection and maximum uptime. You get superior performance at the lowest possible price. Also, with more than 20 years experience and an extensive server range, we know what IT professionals need. Get full root access for complete control. Choose from professional E5 Intel server processors and the latest generation of AMD processors. You will benefit from a high level of innovation with over 1,300 internal product developers. We are a strong global company with 3 billion dollars in annual revenue and over 6,000 employees worldwide.

- ✓ **UNLIMITED TRAFFIC**
  Included at no extra cost
- ✓ **PARALLELS PLESK® PANEL 11**
  for unlimited domains
- ✓ **EXCLUSIVE TO 1&1:**
  Optional SUSE Linux Enterprise Server
- ✓ **MOBILE SERVER MONITORING**
  for Android and iOS devices

Save $480

Server L 4i	NEW: Server XL 12i	NEW: Server XXL 24i
Intel® Xeon® E3-1220	**Intel® Xeon® E5-2640**	**Intel® Xeon® E5-2640**
4 Cores x 3.1 GHz (3.4 GHz Intel® Turbo Boost)	6 (12 HT) Cores x 2.5 GHz (3.0 GHz Intel® Turbo Boost)	2 x 12 (24 HT) Cores x 2.5 GHz (3.0 GHz Intel® Turbo Boost)
12 GB RAM DDR3 ECC	32 GB RAM DDR3 ECC	48 GB RAM DDR3 ECC
1,000 GB HDD (2 x 1,000 SATA)	2,000 GB HDD (3 x 1,000 SATA)	4,000 GB HDD (3 x 2,000 SATA)
Software RAID 1	Hardware RAID 5	Hardware RAID 5
Free choice of CentOS, Debian, Ubuntu, or openSUSE Optional SUSE Linux Enterprise Server		
Unlimited Traffic (100 Mbit/s)	Unlimited Traffic (100 Mbit/s)	Unlimited Traffic (100 Mbit/s)
$99.99 per month	~~$299.99~~ $259.99 per month	$599.99 per month

Parallels
Plesk Panel

1&1®

MEMBER OF
united internet

www.1and1.com

[illegible]

asked to rate the state of U.S. preparedness for an attack on critical infrastructure on a scale of 1 to 10. He responded, "I would say around a 3." The reasons include the inability to rapidly detect and respond to attacks, a lack of cybersecurity standards and a general unwillingness by both private companies and government agencies to share detailed information about threats and attacks. The DOD and intelligence agencies don't share information because they tend to overclassify it, says Hayden. And critical infrastructure providers prefer to keep things to themselves because they don't want to expose customer data and they're concerned about the liability issues that could arise and the damage their reputations could suffer if news of an attack were widely reported.

Edward Amoroso

"The rules of the game are a little fuzzy on what you can and cannot share," says Edward Amoroso, chief security officer and a senior vice president at AT&T, noting that his biggest concern is the threat of a large-scale DDoS attack that could take down the Internet's backbone. "I need attorneys, and I need to exercise real care when interacting with the government," he says.

In some cases, critical infrastructure providers are damned if they do share information and damned if they don't. "If the government provides a signature to us, some policy observers would say that we're operating on behalf of that government agency," he says. All parties agree that, in a crisis, everyone should be able to share information in real time. "But talk to five different people and you'll get five different opinions about what is OK," says Amoroso. Unfortunately, government policy initiatives intended to resolve the issue, such as the Cybersecurity Act, have failed to move forward.

"It was disappointing for us that this nonpartisan issue became so contentious," says Weatherford. The lack of progress by policymakers is a problem for the DHS and the effectiveness of its National Cybersecurity and Communications Integration Center (NCCIC). The center, which is open around the clock, was designed to be the nexus for information sharing between private-sector critical infrastructure providers — and the one place to call when there's a problem. "I want NCCIC to be the '911' of cybersecurity," he says. "We may not have all the answers or all the right people, but we know where they are."

Meanwhile, both the number of attacks and their level of sophistication have been on the rise. Richard Bejtlich, chief security officer at security consultancy Mandiant, says electric utilities and other businesses are under constant assault by foreign governments. "We estimate that 30% to 40% of the Fortune 500 have an active Chinese or Russian intrusion problem right now," he says. However, he adds, "I think the threat in that area is exaggerated," because the goal of such attacks is to steal intellectual property, not destroy infrastructure.

Others disagree. "We've seen a new expertise developing around industrial control systems. We're seeing a ton of people and groups committed to the very technical aspects of these systems," says Howard Schmidt, who served as cybersecurity coordinator and special assistant to the president until last May and is now an independent consultant.

Should THE U.S. STRIKE BACK?

Most best practices on dealing with cyberattacks on critical infrastructure focus on defense: patching vulnerabilities and managing risk. But should the U.S. conduct preemptive strikes against suspected attackers – or at least hit back?

Gen. Michael Hayden, principal at security consultancy The Chertoff Group, and former director of the NSA and the CIA, says the cybersecurity problem can be understood through the classic risk equation: Risk (R) = threat (T) x vulnerability (V) x consequences (C). "If I can drive any factor down to zero, the risk goes down to zero," he says. So far, most efforts have focused on reducing V, and there's been a shift toward C, with the goal of determining how to rapidly detect an attack, contain the damage and stay online. "But we are only now beginning to wonder, how do I push T down? How do I reduce the threat?" Hayden says. "Do I shoot back?"

The DOD is contemplating the merits of "cross-domain" responses, says James Lewis, senior fellow at the Center for Strategic and International Studies. "We might respond with a missile. That increases the uncertainty for opponents."

Ultimately, countries that launch such attacks will pay a price, says Howard Schmidt, former cybersecurity coordinator and special assistant to the president. The U.S. response could involve economic sanctions – or it could involve the use of military power.

ROBERT L. MITCHELL

"People are too quick to dismiss the link between intellectual property loss through cyber intrusions and attacks against infrastructure," says Kurtz. "Spear phishing events can lead to the exfiltration of intellectual property, and that can have a spillover effect into critical infrastructure control system environments."

Spear phishing attacks, sometimes called advanced targeted threats or advanced persistent threats, are efforts to break into an organization's systems by targeting specific people and trying, for example, to get them to open infected email messages that look like they were sent by friends. Such attacks have been particularly difficult to defend against.

Then there's the issue of zero-day attacks. While software and systems vendors have released thousands of vulnerability patches over the past 10 years, Amoroso says, "I wouldn't be surprised if there are thousands of zero-day vulnerabilities that go unreported." And while hacktivists may brag about uncovering vulnerabilities, criminal organizations and foreign governments prefer to keep that information to themselves. "The nation-state-sponsored attack includes not only the intellectual property piece but the ability to pre-position something when you want to be disruptive during a conflict," Schmidt says.

asked to rate the state of U.S. preparedness for an attack on critical infrastructure on a scale of 1 to 10. He responded, "I would say around a 3." The reasons include the inability to rapidly detect and respond to attacks, a lack of cybersecurity standards and a general unwillingness by both private companies and government agencies to share detailed information about threats and attacks. The DOD and intelligence agencies don't share information because they tend to overclassify it, says Hayden. And critical infrastructure providers prefer to keep things to themselves because they don't want to expose customer data and they're concerned about the liability issues that could arise and the damage their reputations could suffer if news of an attack were widely reported.

Edward Amoroso

"The rules of the game are a little fuzzy on what you can and cannot share," says Edward Amoroso, chief security officer and a senior vice president at AT&T, noting that his biggest concern is the threat of a large-scale DDoS attack that could take down the Internet's backbone. "I need attorneys, and I need to exercise real care when interacting with the government," he says.

In some cases, critical infrastructure providers are damned if they do share information and damned if they don't. "If the government provides a signature to us, some policy observers would say that we're operating on behalf of that government agency," he says. All parties agree that, in a crisis, everyone should be able to share information in real time. "But talk to five different people and you'll get five different opinions about what is OK," says Amoroso. Unfortunately, government policy initiatives intended to resolve the issue, such as the Cybersecurity Act, have failed to move forward.

"It was disappointing for us that this nonpartisan issue became so contentious," says Weatherford. The lack of progress by policymakers is a problem for the DHS and the effectiveness of its National Cybersecurity and Communications Integration Center (NCCIC). The center, which is open around the clock, was designed to be the nexus for information sharing between private-sector critical infrastructure providers — and the one place to call when there's a problem. "I want NCCIC to be the '911' of cybersecurity," he says. "We may not have all the answers or all the right people, but we know where they are."

Meanwhile, both the number of attacks and their level of sophistication have been on the rise. Richard Bejtlich, chief security officer at security consultancy Mandiant, says electric utilities and other businesses are under constant assault by foreign governments. "We estimate that 30% to 40% of the Fortune 500 have an active Chinese or Russian intrusion problem right now," he says. However, he adds, "I think the threat in that area is exaggerated," because the goal of such attacks is to steal intellectual property, not destroy infrastructure.

Others disagree. "We've seen a new expertise developing around industrial control systems. We're seeing a ton of people and groups committed to the very technical aspects of these systems," says Howard Schmidt, who served as cybersecurity coordinator and special assistant to the president until last May and is now an independent consultant.

THE U.S. STRIKE BACK?

Most best practices on dealing with cyberattacks on critical infrastructure focus on defense: patching vulnerabilities and managing risk

"People are too quick to dismiss the link between intellectual property loss through cyber intrusions and attacks against infrastructure," says Kurtz. "Spear phishing events can lead to the exfiltration of intellectual property, and that can have a spillover effect into critical infrastructure control system environments."

Spear phishing attacks, sometimes called advanced targeted threats or advanced persistent threats, are efforts to break into an organization's systems by targeting specific people and trying, for example, to get them to open infected email messages that look like they were sent by friends. Such attacks have been particularly difficult to defend against.

Then there's the issue of zero-day attacks. While software and systems vendors have released thousands of vulnerability patches over the past 10 years, Amoroso says, "I wouldn't be surprised if there are thousands of zero-day vulnerabilities that go unreported." And while hacktivists may brag about uncovering vulnerabilities, criminal organizations and foreign governments prefer to keep that information to themselves. "The nation-state-sponsored attack includes not only the intellectual property piece but the ability to pre-position something when you want to be disruptive during a conflict," Schmidt says.

Usually in espionage it's much easier to steal intelligence than it is to do physical harm. That's not true in the cyber domain, says Hayden. "If you penetrate a network for espionage purposes, you've already got everything you'll want for destruction," he says.

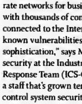
On the other hand, while it's impossible for a private company to defend itself from physical warfare, that's not true when it comes to cyberattacks. Every attack exploits a weakness. "By closing that vulnerability, you stop the teenage kid, the criminal and the cyberwarrior," says Pescatore.

Control Anxiety

Computerized control systems are a potential problem area because the same systems are in use across many different types of critical infrastructure. "Where you used to turn dials or throw a switch, all of that is done electronically now," Schmidt says.

In addition, many industrial control systems that used to be "air-gapped" from the Internet are now connected to corporate networks for business reasons. "We've seen spreadsheets with thousands of control system components that are directly connected to the Internet. Some of those components contain known vulnerabilities that are readily exploitable without much sophistication," says Marty Edwards, director of control systems security at the Industrial Control Systems Cyber Emergency Response Team (ICS-CERT) at the DHS. The organization, with a staff that's grown tenfold to 400 in the past four years, offers control system security standards, shares threat data with critical infrastructure providers and has a rapid response team of "cyberninjas," high-level control systems engineers and cybersecurity analysts who can be deployed at a moment's notice.

Last year, ICS-CERT issued 5,200 alerts and advisories to private industry and government. "[Edwards] had teams fly out seven times last year to help businesses respond to events that either took them offline or severely impacted operations," says Weatherford, who declined to provide details on the nature of those events.


Howard Schmidt

Control systems also suffer from another major weakness: They're usually relatively old and can't easily be patched. "A lot of them were never designed to operate in a network environment, and they aren't designed to take upgrades," Schmidt says. "Its firmware is soldered onto the device, and the only way to fix it is to replace it." Since the systems were designed to last 10 to 20 years, organizations need to build protections around them until they can be replaced. In other cases, updates can be made, but operators have to wait for the service providers who maintain the equipment to do the patching.

So where should the industry go from here?

The place to start is with better standards and best practices, real-time detection and containment, and faster and more detailed information sharing both among critical infrastructure providers and with all branches of government.

While some progress has been made with standards at both the DHS and industry groups such as the NERC, some argue that government procurement policy could be used to drive higher security standards from manufacturers of hardware and software used to operate critical infrastructure. Today, no such policy exists across all government agencies.

"Government would be better off using its buying power to drive higher levels of security than trying to legislate higher levels of security," argues Pescatore. But the federal government doesn't require suppliers to meet a consistent set of security standards across all agencies.

Even basic changes in contract terms would help, says Schmidt. "There's a belief held by me and others in the West Wing that there's nothing to preclude one from writing a contract today that says if you are providing IT services to the government you must have state-of-the-art cybersecurity protections in place. You must have mechanisms in place to notify the government of any intrusions, and you must have the ability to disconnect networks," he says.

But government procurement policy's influence on standards can go only so far. "The government isn't buying turbines" and control systems for critical infrastructure, says Lewis.

When it comes to shutting down attacks, faster reaction times are key, says Bejtlich. "Attackers are always going to find a way in, so you need to have skilled people who can conduct rapid and accurate detection and containment," he says. For high-end threats, he adds, that's the only effective countermeasure. Analysts need high visibility into the host systems, Bejtlich says, and the network and containment should be achieved within one hour of intrusion.

Opening the Kimono

Perhaps the toughest challenge will be creating the policies and fostering the trust required to encourage government and private industry to share what they know more openly. The government not only needs to pass legislation that provides the incentives and protections that critical infrastructure businesses need to share information on cyberthreats, but it also needs to push the law enforcement, military and intelligence communities to open up. For example, if the DOD is planning a cyberattack abroad against a type of critical infrastructure that's also used in the U.S., should information on the weakness being exploited be shared with U.S. companies so they can defend against counterattacks?

"There is a need for American industry to be plugged into some of the most secretive elements of the U.S. government — people who can advise them in a realistic way of what it is that they need to be concerned about," says Hayden. Risks must be taken on both sides so everyone has a consistent view of the threats and what's going on out there.

One way to do that is to share some classified information with selected representatives from private industry. The House of Representatives recently passed an intelligence bill, the Cyber Intelligence Sharing and Protection Act, which would give security clearance to officials of critical industry operators. But the bill has been widely criticized by privacy groups, which say it's too broad. Given the current political climate, Hayden says he expects the bill to die in the Senate.

Information sharing helps, and standards form a baseline for protection, but ultimately, every critical infrastructure provider must customize and differentiate its security strategy, Amoroso says. "Right now, every business has exactly the same cybersecurity defense, usually dictated by some auditor," he says. But as in football, you can't win using just the standard defense. A good offense will find a way around it. "You've got to mix it up," Amoroso says. "You don't tell the other guys what you're doing." ◆

GETTY IMAGES

Time Off TO INNOVATE

Companies like Google and 3M give tech workers free time to follow their passions. Could it work for your organization? **BY HOWARD BALDWIN**

IF YOU'VE USED a Post-it note lately or sent a message from a Gmail account, you've been the beneficiary of a corporate innovation program that gives employees time to be creative — and, while they're at it, sometimes invent products that go on to become wildly popular.

Google is well known for its "20% time," which gives employees a day a week to follow their passions, but it's hardly the first company to offer such a perk. For decades, 3M has allowed employees to devote 15% of their time to innovation — a policy that led to the creation of the now-ubiquitous yellow sticky note, among other products.

Dan Pink, author of the best-selling book *Drive: The Surprising Truth About What Motivates Us*, says hard numbers on corporate innovation programs are difficult to come by, but interest is on the rise. "I do know that more organizations are looking at the

CHECKLIST: HOW TO GET STARTED

Thinking of starting a Google-style "20% time" innovation "time-off" program in your department? Here's some advice from IT managers who have paved the way:

- **Decide what percentage of time the program will include: 20%? 10%? Less?** There are no hard-and-fast rules, and you have to balance employee productivity with the less-restricted idea of innovation.

- **Get management buy-in for any program that consumes a half-day per week or more,** because that would represent a 10% cut in the amount of time employees spend on "real work."

- **Make participation voluntary.** Not everyone in your IT department may want to play.

- **Extend participation beyond developers to the entire IT staff.** Atlassian's biggest payoff came from an idea generated by a QA analyst.

- **Apply some structure and milestones** to ensure that projects don't go on and on without delivering results.

- **Consider how you'll support collaboration.** Will you use digital tools, such as wikis for asynchronous discussions, or actual physical facilities, such as conference rooms where teams can meet in person?

- **Be sure to track all projects,** not just the successes. An idea that didn't bear fruit initially might be worth pursuing later.

- **Consider whether you want to set up a rewards system.** True, you're already paying people to do their jobs, but you might want to think about bonuses if an innovation project results in a huge payoff – like Atlassian's Bonfire did.

- **Manage your own expectations and those of senior executives.** Supporting innovation may not deliver immediate results, and you should feel free to tweak the program based on feedback by the participants.

– HOWARD BALDWIN

companies that are doing it and that it's becoming more popular."

Why? Because otherwise, innovation doesn't happen. "The CEO may say innovation is one of the company's top three priorities," says Doug Williams, a Forrester Research analyst, "but there's always something happening in the short term that pushes the long-term innovation off."

When innovation gets postponed for too long, companies languish — witness RIM's reversal of fortune and Microsoft's vilification in the mainstream media for its failure to innovate. "Innovation programs remove the constraints that accompany traditional work and offer a safe space for failure," Pink says. "That lets people try riskier things."

Time Off Pros and Cons

Sometimes known as innovation time off, or ITO, creativity programs aim to battle stagnation in multiple ways. For one thing, by giving employees the freedom to explore and be creative, they can improve morale and help make individuals more productive in their day-to-day work. And when inspiration strikes, the end result can be a product or internal tool that boosts companywide productivity, increases revenue or both.

Creativity programs also represent a new way to help retain employees in today's competitive labor market. "The old motivational techniques have run their course," says Pink. "We've oversold the carrot-and-stick and undersold quieter forms of motivation."

"It's energizing for employees to take a break from their day-to-day business and think creatively about solving other problems or using technology in a different way," says Williams. "Employees recognize it as something valuable."

None of which is to say there aren't downsides to such programs. For some managers, it's hard to let staffers spend even an occasional half-day on an outside project without expecting immediate results. For employees, it can be hard to shift focus and take up something amorphous when real-world deadlines loom.

But some people who have participated in such programs say the potential for positive results is worth it.

"When I started here, one of the first things I heard was that the IT department had lots of ideas, but few saw the light of day," says Mamatha Chamarthi, vice president and CIO of business technology solutions at Consumers Energy, an electric and natural gas utility in Jackson, Mich. "Having a 20% program lets ideas bubble up," she says. "Sometimes you need to unleash a grass-roots level of passion to generate more innovative and transformational changes."

How Much Time Is Enough?

When setting up an innovation program, one of the hardest decisions to make is how much time should be devoted to it. There is little consistency on this score among organizations that have such programs. The time allotted ranges from a few days per year to one day each quarter to one day per week.

One thing is clear: Because Google's program is so well known, "20% time" has become something of a guiding principle for the way innovation initiatives should be structured, but that's a gold standard that not many employers are able to match. "Some companies simply don't have the luxury to give employees 20% of their week to work this way," says Williams, noting that 10% — about an afternoon each week — may be more reasonable.

And even less-frequent programs can deliver tangible results.

Take the Innovation Days program at the University of Pennsylvania, which was created by Robin Beck, the school's vice president of information systems and computing, to give employees a chance to come up with IT-related improvements of their choice.

"We want to foster innovation and creativity, but the day-to-day reality of delivering IT gets in the way," Beck explains. Officially setting aside time for such efforts shows that innovation is a priority.

The twist? Exploration Days is a three-day event that takes place just once a year. The process begins with IT staffers posting ideas and, if interested, recruiting collaborators on an Exploration Days wiki. Teams and individuals work on their projects on one of two days (in order to provide flexibility). On the third day, dubbed Report Out Day, there's an ice cream social and participants give presentations about what they've achieved.

Beck and her team considered both monthly and quarterly programs before deciding to start with an annual event. The first took place in August of 2011, and a second one was held this summer.

Participation isn't mandatory, but Beck reports that most of her 300 employees participated last year, and last year's projects have born fruit. One team tackled the problem of configuring students' personal devices for the university's wireless network. It developed a simpler process that saves time for both students and IT staffers.

Atlassian, a Sydney-based maker of collaboration software, has two innovation programs: a 20% time initiative and one called ShipIt, which takes place quarterly over 24 hours.

ShipIt starts at 4 p.m. on a Thursday and goes to 4 p.m. the following day. "The idea is to give employees the opportunity to itch something they wanted to scratch," says company president Jay Simons, adding that employees can work solo or in teams, usually of no more than five.

Projects can be a prototype of a new feature or a fix to an existing product, but whatever it is, it has to be completed in 24 hours. "By compressing the time, it made the innovation target more bite-sized and achievable," Simons explains.

Another key requirement: The results of ShipIt work must be presented to co-workers in a five-minute demo. "Even if someone tried to build a widget and failed, they have to give a presentation," says Simons. "Because then, five people will go up to that developer afterwards and offer ideas."

Only about one-third of the company's 500 employees — mostly engineers — participate in the 20% program "because it's hard to dedicate a day a week to something," says Simons. "Products have to ship, and sometimes development takes longer than estimated."

Payoffs

The benefit of having two programs is that each serves a different purpose, according to Simons. The ShipIt program has been the source of "hundreds of small improvements to business processes," he says. The 20% time initiative, on the other hand, has yielded fewer results, but those results have had a big impact.

How big? One 20% time program evolved into an open-source JavaScript-based graphic manipulation tool called Raphael.

And in another 20% time project, a quality assurance engineer — not even a software developer — built a prototype of an internal bug-tracking system for the company's JIRA software, which tracks software development projects. The result was so impressive that Atlassian turned it into a product, Bonfire, which started shipping in July 2011. Total revenue at last tally: $1 million, and the QA engineer is now its product manager.

Not all innovations pay off quite so handsomely, or yield any monetary return at all — nor are they designed to.

At Detroit-based online mortgage lender Quicken Loans, CIO Linglong He oversees a program called BulletTime (so named because the projects are quick and targeted). The idea is for all 750 IT team members to take time to work on personal projects every Monday from 1 p.m. till the end of the workday.

Notable BulletTime projects include an internal application called Qwicktionary that lists all of the abbreviations used by the company; a mortgage calculator for clients; and an iPhone app called NorthStar that indicates the location of the company's 100-plus conference rooms. "NorthStar had a positive impact on meeting productivity, because people aren't late to meetings anymore," says He.

Set Parameters

Allowing something as amorphous as time out to innovate may be anathema to some IT organizations and managers, but supporters say techies are uniquely suited to such programs. "Innovation and creativity are an important part of what any IT organization does," says Penn's Beck.

That said, ITO programs need guidelines. Consumers Energy has internal communications tools, such as Yammer, that employees use to post ideas and form teams. Chamarthi and her staff meet weekly to review the ideas. If the business side likes a project enough to fund it, it has to reduce the priority of another project. The underlying message to the IT team: 20% projects have to have business value.

And no matter what the goal, CIOs advise patience when it comes to implementing innovation programs. "You have to set the expectations that this is an experiment and it may change along the way," says He. "You also have to build flexibility in. Too often, technology leaders want to build a perfect solution from day one."

Finally, warns Beck, if innovation and creativity are not part of your existing culture, you're not going to instill those qualities in a single day. "It has to be something you encourage on a consistent basis," she says. "Be patient. You're planting seeds, and it can take time for ideas to germinate." ◆

Baldwin *is a Silicon Valley-based freelance writer and a frequent contributor to* Computerworld.

THINKSTOCK

[WHY PASSWORDS STILL FAIL US]

Passwords aren't working, and replacement technologies haven't caught on. Why can't we develop a simple way to secure our data? **BY HOWARD BALDWIN**

PASSWORDS WEREN'T THE ONLY FAIL in last summer's widely publicized "epic hack" of tech journalist Mat Honan — Amazon, Apple and, to a lesser extent, Google and Honan himself share the blame.

But passwords played a part in the perfect storm of user, service provider and technology failures that wiped out Honan's entire digital life. As he concluded in his account of the hack, "Password-based security mechanisms — which can be cracked, reset and socially engineered — no longer suffice in the era of cloud computing."

The problem is this: The more complex a password is, the harder it is to guess and the more secure it is. But the more complex a password is, the more likely it is to be written down or otherwise stored in an easily accessible location, and therefore the less secure it is. And the killer corollary: If a password is stolen, its relative simplicity or complexity becomes irrelevant.

Password security is the common cold of our technological age, a persistent problem that we can't seem to solve. The technologies that promised to reduce our dependence on passwords — biometrics, smart cards, key fobs, tokens — have all thus far fallen short in terms of cost, reliability or other attributes. And yet, as ongoing news reports about password breaches show, password management is now more important than ever.

All of which makes password management a nightmare for IT shops. "IT faces competing interests," says Forrester analyst Eve Maler. "They want to be compliant and secure, but they also want to be fast and expedient when it comes to synchronizing user accounts."

Is there a way out of this scenario? The answer, surprisingly, may be yes. There's little consensus on what the best solution will be, but consultants and IT executives express optimism about the future. They cite technologies such as single sign-on, two-factor authentication, machine-to-machine authentication and better biometrics as ways to strengthen security — eventually. For now, each still has its drawbacks.

The Problem With Passwords

Despite years of well-publicized breaches, weak passwords still subvert IT security, but the most obvious solution — strong passwords — comes with its own set of problems.

Complex passwords annoy or stymie users, who subsequently take up IT's time asking for password resets, thereby lowering productivity for both groups. The result, laments Maler: "IT ends up with both a lack of usability and a false sense of security."

What's more, both weak and strong passwords are vulnerable to human error. Among other things, they may be written down, stored in visible places online or on personal devices, shared with friends and co-workers, or divulged via phishing schemes.

It's a problem with old roots. Security expert Larry Ponemon of the Ponemon Institute worked on a project some 15 years ago for a government agency that required users to create 15-character passwords and update them every 30 days.

"If you forgot your password, you had to go to a tyrant at the help desk who would call you incompetent before he'd reset your password," Ponemon remembers. "When I walked through the office, I saw that all these employees working on highly confidential documents had written their passwords on Post-it notes because they didn't want to deal with the tyrant."

At Case Western Reserve University in Cleveland, CISO Tom Siu has seen it all: professors giving passwords to teaching assistants and TAs sharing them with peers. Siu recently traced an unauthorized software download to the ex-boyfriend of a former student.

SINGLE SIGN-ON FOR THE ENTERPRISE

Several enterprise password management tools offer dual-factor authentication along with single sign-on and other security capabilities, such as compliance features. Options include the following:

ManageEngine's Password Manager Pro

Thycotic Software's Secret Server

Splash Data's SplashID Enterprise Safe

Lieberman Software's Enterprise Random Password Manager

As our lives proliferate online, the sheer number of passwords that any one person is required to use becomes a problem. The Ponemon Institute conducted a study several years ago to determine how many passwords people could remember. For most people, it was one or two; some could manage three.

"That means you have a top-secret password for your bank," plus one other password "for everything else," says Ponemon. "If someone steals [the latter], they can probably get other challenge and verification information, like the name of your first-grade teacher."

And, despite IT's best efforts, users continue to fall for phishing attacks. "When we educate people about phishing, the number of people who fall for it goes down," says Jonathan Feldman, director of IT services for the city of Asheville, N.C. "But it never goes down to zero."

And then there are hackers. Even strong passwords can be stolen in batches, as multiple high-profile cases have shown.

All of which makes a strong case for a Plan B.

Short-term Solutions: SSO and LDAP

In the short term, Plan B to many IT executives is single sign-on (SSO) technology or the Lightweight Directory Access Protocol (LDAP).

Single sign-on, as its name implies, lets users log in once and then authenticates them for multiple systems. LDAP, which runs on IP networks, works with Microsoft's Active Directory to allow any application using Active Directory to accommodate the same password.

Forrester's Maler notes that one of the big advantages of single sign-on is that it eliminates the need to have multiple systems storing multiple passwords. Ponemon concurs, citing a recent SSO deployment at a healthcare provider where practitioners were complaining about how they had to type in their password every time they moved to a different system. "The SSO system created both efficiency and greater security, because it had built-in safety checks to avoid giving access to the wrong person."

While acknowledging that neither SSO nor LDAP is perfect, Paul Capizzi, who recently left his post as vice president of IT at New York-based insurance firm SBLI USA, says they're better than the alternative. Capizzi says SBLI users generally manage up to a dozen passwords, and if they regularly call the help desk for password resets, that's a waste of time for everyone.

For that reason, most of SBLI's recent upgrades included adding LDAP and single sign-on support. "We'll never turn down the opportunity to use LDAP," he says. "We're always looking for ways to leverage that, because it increases users' performance."

One LDAP drawback: Many legacy systems can't support Active Directory, which means a separate password is still necessary for those systems.

"We still have a mixture of Windows-based applications and custom applications that were never designed to acknowledge the existence of AD," says a retail industry IT executive who asked that his name not be used. "Getting them to talk to each other is an investment of time and money, and it's not always our highest priority."

Feldman, meanwhile, points out that SSO has drawbacks of its own. "If your password gets compromised in one place, it's compromised everywhere," he says.

If an SSO system is breached by a phishing expedition, the hackers can then go to the website and try passwords to get to other parts of the system, he explains. Or they can start probing for an IP stack or a GRE (generic routing encapsulation). Instead of SSO, Feldman uses digital security certificates to limit the city's vulnerability.

Overall, SSO makes users' lives simpler and LDAP makes security administration easier. They're not perfect, sources agree, but together, they do provide some interim value.

Biometrics

Other highly touted security technologies continue to evolve, but at a pace that's too slow for most IT managers. And the newer technologies have flaws of their own.

For example, smart cards aren't widely deployed but are frequently used in highly secure installations. Earlier this year, however, the smart-card readers at the Department of Defense were breached by malware that sniffed the PINs on smart cards. "It was kind of like protecting a nuclear facility with a house key," says Maler.

Nor has biometrics taken off — yet. The most extensive deployment of biometric technology is in fingerprint readers on Lenovo ThinkPads, which SBLI used for a while. It was a cool feature until the sensors got dirty and it started taking six swipes before the system recognized the user's fingerprint, according to Capizzi.

"Some people said it worked great, but others found it more annoying than typing in a password," he says, noting that the readers also made the laptops more expensive. "From a corporate perspective, I'm not sure biometrics is there yet."

Nevertheless, the retail industry IT executive says he plans to investigate biometrics for a legacy point-of-sale system that can't be integrated with Active Directory. "Our salespeople aren't assigned to a register. Instead, there are multiple POS terminals throughout the store, so they're logging in and out often." He says he'd like to retrofit the POS terminals so employees can access the system with the tap of finger, noting that it would be an improvement over users mistyping passwords or forgetting them altogether.

Security consultant Ponemon holds some optimism for biometrics — although he chuckles at instances like the botched Department of Homeland Security installation at the border crossing at Nogales, Ariz., where the scanner was installed upside down and failed everyone who tried it. "Implemented correctly, some biometrics systems are really cool," he says. "The Israelis have created very robust voice-recognition tools that can determine identity within a nanosecond."

He says he believes that voice recognition tools will be more viable than facial recognition, fingerprint or iris scanning systems. "People are too nervous" about having their eyes scanned, he points out.

Feldman says he's investigated almost everything under the sun. He's not bullish on biometric tools because he's seen too many of them fail. He's not keen on key fobs (which display a one-time access code after the user enters a PIN) because they have to be discarded after a few years, and because he doubts that users would report lost key fobs. And after the breach of EMC's RSA security division last year, he's not convinced that the vendor's method of displaying access codes — on a USB-based hardware token — is viable either.

Cellphones to the Rescue?

That doesn't mean Feldman is down entirely on device authentication, which strengthens the password updating process by using a second trusted channel of communication in addition to a primary network connection. Feldman is looking at using cellphones as the secondary channel. "Everyone's got a phone," he reasons.

Instead of an access code displaying on a hardware token, it would appear in an SMS or text message on a phone. Users wanting to log in to a data center, then, would enter both their password and the randomly generated access code received via their phone.

Forrester's Maler also likes this idea. "IT generates a new, one-time password and provisions it to the enterprise user by means of an alternate channel — in this case, the carrier network. That's really powerful, because it's part of a password policy that forces change, and it's strong authentication because it involves something you know — the password — and something you have — the computing device."

Case Western's Siu is even more enthusiastic about device authentication. "It'll keep people from sharing credentials, because for that to work, someone has to hand over their phone, and no one wants to do that," he says. The increasing popularity of smartphones improves the feasibility of this method.

Ponemon agrees, and adds that devices even smarter than smartphones may improve security. He believes device recognition technology, where the system recognizes your computer based on its IP address and other recognizable factors, will take hold, especially with security capabilities being built into processors. "It's technology that will get people in and out of systems safely," he says. "Computers with these chips will be low cost, but they'll be useful in a wide array of scenarios."

Whatever device-based technology wins, it will involve a set of checks and balances. "We'll always have password problems," acknowledges Siu. "While users always want a single place to log in, we're going to need multiple levels of authentication." He anticipates that in the future we'll carry something that authenticates us, perhaps our phone or something with an RFID tag, the just as a highway toll transponder authenticates a car at a toll booth or a key fob lets you start a Prius when it's in the vicinity.

Ultimately, even the security experts are optimistic. "We're at a turning point in the security industry," insists Ponemon. "There are lots of venture capital investments looking at this facet of security. It's a response not just to [breaches at popular sites such as LinkedIn], but to hackers in China and Russia who are looking for weaknesses."

With the threat vector high, so too is the likelihood of a successful technological response. In the meantime, IT will keep on trying to exhort users to choose stronger passwords — and that includes their own systems administrators. As Maler relates, a recent Forrester study found that the most common administrator password for Microsoft Exchange is — you could have guessed it — password1. ♦

Baldwin *is a frequent* Computerworld *contributor.*

Security Manager's Journal

MATHIAS THURMAN

A Reality Check for Maturity

An assessment of the information security department shows that it still has a lot of growing up to do.

I THOUGHT I was a security adolescent, but I'm really just a toddler.

Many IT managers can probably tell from that statement that I have been looking into maturity models. I did that at the request of our CIO, who asked all of his department managers to develop a maturity model and identify where we are. Perhaps the topic came up at a conference he attended, but no matter; I had never assessed the maturity of my department at my current company.

My first step was to turn to the Internet to try to find the maturity model that could best help me measure our security program against industry standards. I wanted something that would let me communicate the level of our security maturity in one slide.

I soon found that there are a lot of models to choose from. They range from the complex, requiring lengthy calculations and surveys, to the fairly simple.

Taking into account time and resources, I chose the Gartner Security Maturity Model, making a few modifications of my own. The Gartner model segments maturation into phases: Blissful Ignorance (or what I call the initial phase), Awareness (or the developmental phase), Corrective Action (or the define and manage phase) and Operational Excellence (or the optimized phase). According to Gartner, about half of all companies are in the Awareness phase, and only 5% ever reach Operational Excellence. In other words, most companies know where their weaknesses are but are not yet taking action to correct them.

[illegible] computerworld.com/blogs/security

As I worked my way through the questions that Gartner provides to help clients position themselves on the maturity scale, it became painfully obvious that my security program is not as advanced as I had thought.

Sure, we've spent a lot of money deploying some of the standard buzzword technologies: SIEM, DLP, NAC, file encryption, IPS, content filtering, multifactor authentication, spam filtering, endpoint protection. I have developed a comprehensive set of policies based on ISO 27001 and created awareness training as well as various procedures and processes. But with many of these technologies, we are still in our infancy in terms of capabilities, coverage, deployment and user acceptance.

> It became painfully obvious that my security program is not as advanced as I had thought.

Trouble Ticket

For example, while we have deployed data leak prevention technology (that's the "DLP" in the list above) to detect when key documents leave the company, we have not enabled prevention or blocking features; we can monitor but not prevent. We also lack network sensors in every office, leaving gaps in coverage.

Then there's our network access control (NAC) deployment. We have rolled that out only to large offices — and not even to all of those — and we currently monitor only for devices connected to the network. We haven't yet enabled the enforcement of NAC, since we're still tuning the deployment and dealing with exceptions and other challenges related to mobile devices and nonstandard systems.

On the other hand, some of our security technologies are fully mature. Our firewalls have intrusion prevention enabled and actively block malicious traffic. We also enable URL filtering on our firewalls to block access to sites that represent legal or security risks.

But when I step back and evaluate our security landscape, I realize that we're still very much in what Gartner calls the Awareness phase — in fact, my honest assessment is that we're in the lower quadrant of that phase.

My goal for 2013 is to accelerate the security program by enforcing policies, and thereby move us closer to joining that magical 5% of companies that have achieved Operational Excellence. For now, that's a pipe dream, but it's a worthy goal. ◆

This week's journal is written by a real security manager, **"Mathias Thurman,"** *whose name and employer have been disguised for obvious reasons. Contact him at mathias_thurman@yahoo.com.*

INSERT
EFFICIENCY
HERE

BART PERKINS

Change Management Is Not Optional

You can't assume that if you just design a better approach, people will embrace it.

HIGH-IMPACT PROJECTS — those aiming for streamlined, redesigned and transformed business processes — require more than incremental change. But few people embrace change enthusiastically. Staff can be stiffly resistant to new processes, interfaces or job responsibilities. It's a challenge that calls for effective change management.

Unfortunately, even multinational enterprises often ignore change management until problems arise. Many good project teams naively assume that if they just design a better approach, people will automatically embrace the new system. (I'm still waiting to see this happen in the real world.)

Other reasons that projects often neglect change management include tbe following:

Incomplete analysis. Lacking a full understanding of job content and interactions, project teams might not see the need for change management. Analysts at one large manufacturing company decided that field repair technicians should be able to complete more tban their current 3.2 service calls per day. To that end, the analysts decided that techs no longer needed to start their day at the supply depot. Instead, supplies would be shipped directly to the techs, transforming each truck into a mini warehouse. Result: Calls completed per day decreased sharply. The analysts had failed to understand the flow of critical information. Techs routinely shared their diagnostic and repair experiences with one another during their time at the depot. Without this forum for sharing information, the techs were less effective and required formal training.

Resource constraints. Change management requires time and money and might be deemed wasteful. This was true at one Fortune 500 company, where the extremely powerful accounting department regularly put project plans through four or five rounds of cost cutting. Project teams that saw value in change management had to create small additional projects (which received less scrutiny) for training, documentation and change management. Unfortunately, this approach resulted in out-of-sync schedules and poor integration among other project activities, severely hampering change management efforts.

Politics. Teams might be reluctant to challenge entrenched interests. A state governor announced a program to implement common systems across all state agencies. The project team recognized that the resulting new business processes and job content would be so different that the only hope of success lay in a massive change management effort to get buy-in from the people who would use the new system. They were confident that, given enough time for communication and training, workers and middle managers would embrace the changes. Unfortunately, prior governors had allowed each agency to build its own IT capability, and none of the agencies wanted to relinquish IT staff and funding. Since the governor was unwilling to confront the entrenched bureaucracy, the team backed off and eventually reproduced each agency's legacy package in the new system. The governor declared success, and the bureaucrats retained power.

Successful projects require organizational acceptance to achieve their full potential. Even otherwise well-designed projects often fail when change management is neglected. Be proactive! Require high-impact projects to include a change management analysis and plan. Otherwise, you risk impacting your project's acceptance, business benefits and ultimate success. ◆

Bart Perkins is managing partner at Louisville, Ky.-based Leverage Partners, which helps organizations invest well in IT. Contact him at BartPerkins@LeveragePartners.com.

Career Watch

ASK A PREMIER 100 IT LEADER

Jacqueline M. Lucas

The CIO at Baptist Healthcare System answers questions about having your **suggestions taken seriously** *and more.*

I'm always making suggestions, almost all of which are ignored by my boss. I've been here long enough that we have started implementing some of the things I suggested years ago, but only because everyone else now does things that way. I feel frustrated. I don't want to be a manager myself, but boy, would I like to be the guy who makes decisions! What I'm wondering about right now, though, is whether I could learn to be more influential or if I just need a new job and a new boss. You should consider how you are presenting your suggestions. Are you tossing them out casually with little preparation? Are you offering to help champion, manage or implement suggestions or just throwing them out, hoping the supervisor will take them on and make them happen?

My recommendation is to vet each suggestion with colleagues before presenting them, to assess their feasibility. Then prepare a brief document outlining the suggestion and how it could be accomplished and present it to the boss with an offer to participate in the implementation. This sends the message that you are serious and have done your homework, and it should elicit a response.

You have to understand that there are circumstances that can prevent a manager from implementing a recommendation – applicability, risk aversion, monetary restraints, competing priorities, etc.

And, of course, the decision to leave a position is a major one and should be made based on many factors, including career path, job market, location and family needs.

I often have to work with a very negative person. I deflect the complaints as best I can, but it actually wears me out to be with him. What can I do? One approach would be to take the co-worker aside and, in a caring manner, say that it's obvious that he's unhappy and that you'd like to know how you could help make things better. This will not only open up a dialogue but also let your co-worker know that his attitude is noticeable. Sometimes people don't even realize how they are perceived. However, you must be ready to listen to the person and offer some constructive solutions and assistance.

What has been most helpful to you in your career: education, experience or people? Can I choose all of the above? All three have played major roles in my career at different times, with education dominating early in my career and experience and relationships with people being more important most recently.

If you have a question for one of our Premier 100 IT Leaders, send it to **askaleader@computerworld.com**, and watch for this column each month.

The Outside-the-Box Job Interview

Here are some tips for your next IT job interview, from John B. Molidor and Barbara Parus, authors of *Crazy Good Interviewing: How Acting a Little Crazy Can Get You the Job.*

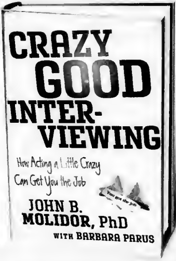
1 **Show your analytical side.** Create a presentation on your iPad illustrating how you saved a previous employer money and/or time by recommending a software product or a new system.

2 **Flaunt your "app-titude."** If you created an app for a former employer, show it off.

3 **Make a mock-up.** Present an idea for an app that would benefit your prospective employer's organization.

4 **Critique the employer's website.** Make some positive observations, and then add a couple of suggestions for improvement that would ease navigation or drive sales.

5 **Be enthusiastic and talk as if you already have the job.** For example, if the interviewer mentions a new implementation, say, "When can we get started?" One successful job candidate insists this strategy has resulted in several job offers.



Interested candidates send resume to: Google Inc., PO Box 26184 San Francisco, CA 94126 attn Lisa Harrington Please reference job # below

Test Engineer (Kirkland, WA). **#1615.4027**. Design, develop, modify, and/or test sw needed for various internet search engine co projects Exp incl: manage prod lifecycle, translate func specs, design creation, implement syst in oo lang, dvlp test frmwrks, test large complex prod, web svcs, & appl servers

Software Engineer Positions (Kirkland and Seattle, WA) Design, develop, modify, and/or test sw needed for various internet search engine co projects Exp Incl.,

#1615.4797, Perl, Java C# or C++, oo prog & AJAX, XML, HTML, Web Svcs Frameworks & databases

#1615.4042: large scale data syst design. mach learn, data mine algorithms design & implement sw syst & data models

Interested candidates send resume to: Google Inc., PO Box 26184 San Francisco, CA 94126 attn: Lisa Harrington. Please reference job # below:

Senior Technical Account Mgr (Mountain View, CA) **#1615.1071**: Manage technology programs for Google Exp incl: hw eng'g dvlpmnt, script lang, create presentations, spreadsheet models & process documents; & cross-funct teams that span offc locations, countries & comp: silicon chip & sw eng'g dvlpmnt processes; cryptograph principles & conventional cryptograph algorithms; internet ntwrk topographies & mgmnt protocols; standard comp hw & sw arch. & website dvlpmnt

Developer Programs Engineer (Mountain View, CA) **#1615.1913**: Design, develop, modify, and/or test software needed for various internet search engine company projects. Exp incl Java, PHP Python Ruby, .NET or Jscript; XML, SOAP or REST web svc & web appl &/or mobile appl dvlpmnt Up to 15% trvl req'd

Test Engineer (Mountain View CA) **#1615.4676**: Design, develop modify and/or test hardware needed for various Google projects Exp incl C, C++, Java or Python, create test plans. Unix & Linux, & debug test failures

Mechanical Engineer (Mountain View, CA) **#1615.599** Design and build software, hardware computing platforms and networking technologies. Exp incl thermal design & simulation thermal design of electronics, prod design & dvlpmnt exp. & struct analysis, incl modal random vibration, seismic & fatigue analysis & testing

Program Manager (Mountain View, CA) **#1615.1524**. Manage technology programs for Google Exp incl oper/data-center infrastruct in multi-tiered distrib env proj mgmnt & schedule & full life cycle of prod f/ NPI to EOL

SW Eng Positions (Mountain View, CA): Design, develop modify, and/or test sw needed for verious internet search engine co projects Exp incl:

#1615.2462 data struct & algorithms, C++ & Java program, design patterns; test driven dvlpmnt, TDD, HTML, CSS Jscript AJAX & XML, SQL, script lang design & data analysis, online ad syst. map-reduce, & scalable distrib syst

#1615.759 design patterns, program paradigms, algorithms & data struct: oo lang incl C++ & Python, distrib syst design, distrib comput, & parallel prog principles & models sw testing Unix/Linux, & internationalization issues

#1615.855. large scale prod env oo design patterns develop sw in Java or C++, source control mgmnt syst build env, script lang such as Perl or Python dvlpng sw tools and unit test

#1615.980 C & C++; Java, dvlpmnt of monitor tools f/enterprise-scale data ctr deployments: Linux kernel dvlpmnt; hw disk & virtual disk deployments over native Linux Kernel-based Virtual Machines or the Xen Hypervisor: scalable ntwrk attached disk storage; & disk share Quality of Service algorithms

#1615.4486, AJAX tech: HTML, CSS Jscript jQuery, dvlpmnt in server-side tech, incl Java & C++ ; web appl dvlpmnt; cross-browser pltfrms, oo program, web server admin, code review; & UI dvlpmnt

Interested candidates send resume to: Google Inc., PO Box 26184 San Francisco, CA 94126 attn. Lisa Harrington Please reference job # below

Research Scientist (NY NY), #1615 2193 Research, develop and test Google products Exp incl C; C++, stat model: speech process mach learn & research in speech recognition

SW Eng Position (NY, NY) Design, develop modify, and/or test sw needed for various internet search engine co projects Exp incl

#1&15 4524 C++ & STL. Linux, adv algorithms & data struct; oo design stats & data analysis large distrib syst parallel program, high-perf ntwrkng & storage & low-level perf optimization

#1615 3388 syst-level design scalable components, distrib syst, and technical leadership

#1615 779 AI, data mine text mine natural lang process, computational linguistics, or mach learn info extract & relation extract from free unstruct text on web, prog lang, incl C, C++ Python & Java large-scale syst sw design & dvlpmnt, & sw localization & internationalization

#1615 1864 C++, Java, Jscript, or Python data analysis, oo tech algorithm dvlpmnt & implement, sw implement design & implement of web appl draft tech design docs, & dvlpmnt code & automatic tests

Practice Engagement Manager (Full-Time, Multiple Openings) - Infosys Limited is in need of Practice Engagement Manager(s) to work in Plano, Texas and various unanticipated locations throughout the U.S. to support the creation of sales plans, provide collaterals references and support in prospecting to client services teams navigate the account to identify different kinds of deals, be part of integrated pursuit team help pursuit team with account context and techno-functional review of artifacts required for increasing the service offering, practice footprint in the account: create menu of pricing options and provide Go/No-Go recommendations. Travel Required We are an Equal Opportunity Employer M/F/D/V Please apply on-line at http://www.infosys.com/careers/apply-now/us-jobs.asp and search for the reference # Inf_EXTERNAL_59113125_2

Interested candidates send resume to Google Inc., PO Box 26184 San Francisco, CA 94126 attn. Lisa Harrington Please reference job # below

Product Mgr Position (San Bruno, CA): Take responsibility for Google product from conception to launch. Exp incl

#1615.499 enterprise or consumer prod mgmnt/prod dvlpmnt, collect user reqmnts for dvlpmnt of prod plan & vision bus model, analysis, & predictions, & coordinate cross-funct teams across groups such as mrktng, prod dvlpmnt & policy/legal Up to 20 % trvl req d

Interested candidates send resume to: Google Inc., PO Box 26184 San Francisco CA 94126 attn Lisa Harrington Please reference job # below.

Technical Solutions Engineer (Mountain View CA) **#1615.4485**. Provide technical and product services for Google Exp incl algorithms, data struct; HTTP, J2EE high speed message TCP/IP, database syst C++ & Java

Lead Partner Solutions Specialist (Mountain View CA) **#1615.3671**. Take responsibility for Google product from conception to launch Exp incl mgmnt consult, design partner launch & partner support process, implement strategic proj to improve business efficiency, such as improved cost savings better cust/partner interact models & organization design changes proj mgmnt; people mgmnt & sw dvlpmnt or prod mgmnt Up to 25% trvl req'd

Product Marketing Manager (Mountain View CA). **#1615.586** Manage Google product marketing campaigns Exp incl online mktng online video & audience dvlpmnt, default search homepages, toolbars, & mobile appl & mgmnt online co-mktng & affiliate mktng campaigns.

SW Eng Positions (Mountain View CA) Design, develop modify and/or test sw needed for various internet search engine co projects Exp incl

#1615.2364 C++, tech design & arch, concurrent sw; & 3D comp graphics

#1615.2325 embed syst sw C, C++ & Java, syst sw debug; Linux op syst; web browser tech audio/video pipeline & Android op syst

#1615.2410, C++ mach learn: data mine & analysis oo tech, statistics; syst design, info retrieval algorithms & data struct & MapReduce on Hadoop

#1615.829 C++ Unix comp vision; mach learn' oo prog lang & distrib & parallel compute

#1615.2201, eng'g &/or proj lead. mgmnt lifecycle of prod from reqmnts to user adoption, incl reqmnt gathering translation of funct specs & creation of designs implement of syst in oo lang & API design Up to 25% trvl req'd

#1615.3135, C++ syst-level coding, sw design execute & debug large-scale distrib storage & file syst, large-scale distrib syst perf analysis & tail-latency root cause diagnosis

#1615.3188, distrib compute NoSQL databases MapReduce, scalability; Java Prog multithread, JVM internals java compilers data struct, Jscript Web Prog. incl Jscript compile obfuscation & CSS minimize sw design incl design patterns, testability dependency injection & backward compatibility algorithms HTTP load balance caching & perf & 3rd party ecosyst. incl open standards JSON, markup and schema org

#1615.932, C, C++ Java Python Eclipse Vim, or EMacs, *nix syst & shell script data struct algorithms design patterns, oo program Unix or Linux, build ntwrk-based sw svc syst, data mine, prog lang database op syst comp graphics & human-comp interaction

#1615.4239, oo program & design patterns gameplay eng'g game mechanic design & implement, dependency injection framewrks profile & monitor tools scalable fault tolerant & performant designs & solutions, HTTP JSON & XML, distrib data struct, incl hash tables & consistency, asynchronous program & multithread or concurrency arch, distribute or cloud compute & svc oriented arch

#*315.694 C++, parallel & distrib comput: distrib syst prog, IRP, ntwrk mgmnt, & router & switch arch

ARMO has consulting oppties for S/W Engineers Programmers Business and System Analysts App Developers Tech Leads Project Managers w/Bachs. or Masters degrees and with no experience or with relevant experience in one or more tech's depending on specific position and seniority of the position

If experience is required relevant tech's include Oracle SQL Server ETL, informatica, SAP Peoplesoft, CRM SIEBEL, EAI Business Objects, .NET C#/VB/ASP AJAX Java/J2EE Any suitable combination of edu & exp equal to Masters is acceptable Travel to client sites all over U S for extended periods on short notice is required Salary & benefits competitive based on position and exp. Fax Resumes to 973-215-2151 or email hr@armo-solutions.com or mail to ARMO Consultants, 900 Lanidex Plaza, Suite 240 Parsippany, NJ, 07054

Research in Motion Corporation (US) Andover MA, positions are available

MA7020 – Software Developer

Research in Motion Corporation (US), Cary, NC, positions are available

NC7021 – Software Developer

Research in Motion Corporation (US) Rolling Meadows, IL, positions are available

IL7022 – Antenna Designer

Research in Motion Corporation (US), Irving, TX, positions are available

TX7023 – Wireless Protocol Software Developer

Research in Motion Corporation (US), Redwood City, CA positions are available

CA7029 – Patent Agent

Submit resume to Research in Motion Corporation (US), to P.O Box 141394 Irving, TX, 75014-1394 U.S.A., referencing appropriate job title and requisition number

Computer Professionals for FL based IT Firm: Sr SAP Consultants to Plan, design develop test enhance customize & co-ordinate activities to implement adv s/w module components in complex SAP & ABAP environments. Experience in diff modules of SAP Customization & integration etc Willing to travel & relocate as & when reqd Apply w/2 copies of resume to HR, Auritas, LLC 4907 International Parkway, Ste#1051, Sanford, FL 32771

Interested candidates send resume to Google Inc PO Box 26184 San Francisco CA 94126 attn Lisa Harrington. Please reference job # below

Software Engineer Position (San Francisco, CA) Design, develop modify, and/or test sw needed for various internet search engine oo projects Exp Incl.

#1615.2909 C++ dvlpmnt stat analysis hypothesis test & applied research knwldge representation & semantic process leader of dvlpmnt efforts process terabytes of data design & execute mach learn experiment, & dvlpmnt in distrib parallel process frmwrks Up to 20% trvl req d

Interested candidates send resume to Google Inc., PO Box 26184 San Francisco, CA 94126 attn: Lisa Harrington. Please reference job # below

Business Systems Integrator Positions (Mountain View, CA) Design analytical solutions that provide data to answer complex business decisions. Exp incl

#1615.3230: PL/SQL, Unix, TCP/IP, Avaya PBX, CMS, & IVR; VoIP: data analysis, database admin, ntwrk admin, & design, plan, implement, & support traditional & IP based call ctr solutions, incl CTI, IVR & reporting

#1615.4562: Java, data analysis, oo tech, algorithm dvlpmnt & implement, QA& test, proj mgmnt, & tech presentations

Strategic Planning Manager (Mountain View, CA) **#1615.1116**, Execute high level business operations and strategy projects defined by Google's executive team. Exp incl: consult, incl econ analysis & finan model, analyze data, model finan & oper scenarios, & solve related prob; econometrics, hypothesis test, & survey design; Excel model, incl dvlpng macros, using pivot tables, write array funct, & utilize dynamic ranges, use stats analysis sw. Up to 15% trvl req'd

SW Eng Positions (Mountain View, CA) Design, develop, modify, and/or test sw needed for various internet search engine co projects. Exp incl:

#1615.3433: C or C++; multithread, distrib syst, algorithms & parallel & distrib computing

#1615.2567: Java, Jscript; Linux or Unix, design & implement large-scale distrib sw syst, appl of security & authentication protocols. pltfrm harden & test; & large-scale prod sw syst troubleshoot

#1615.4558, oo design &/or oo prog, LBS technology & geographic map, Linux dvlpmnt, design & maint of large scale distrib syst, & technical leadership of sw dvlpmnt proj

#1615.1883: write sw for Linux in C++ & Python, dvlpmnt of Gentoo-based distrib build syst infrastruct & dvlpr tools, dvlpmnt of Gerrit-based commit queue; distrib of prebuilts via Git, distrib of toolchain upgrades, automation of dependency verify for ELF binaries, optimize of Portage package manager: usage of Linux cgroups to sandbox build processes, automated deduplication of prebuilts & automatic revving of ebuilds in Git.

Interested candidates send resume to: Google Inc., PO Box 26184 San Francisco, CA 94126 attn: Lisa Harrington. Please reference job # below:

Quantitative Analyst (Mountain View, CA) **#1615.3792**: Research methods for improving search engine company technology. Exp incl: data mine; analysis of large data sets using R & SQL; & quantitative analysis & model.

Software Engineer in Test (Mountain View, CA) **#1615.724**: Design, develop, modify, and/or test software needed for various internet search engine company projects. Exp incl: C++, Python, or Java; Linux or Unix; oo dvlpmnt; data struct; algorithms; unit test; & implement, test, maint, & design of backend & frontend subsist.

SW Eng Positions (Mountain View, CA) Design, develop, modify, and/or test sw needed for various internet search engine co projects. Exp incl

#1615.3837, C & C++; oo analysis & design, design & implement of large, highly distrib & reliable syst, Unix or Linux, multicore & multithread, remote proced calls, adv algorithms, concurrency, synchronization, distrib syst, load & perf test, test automation, info retrieval & data mine & database internals

#1615.1288: Python: Bourne Shell: web dvlpmnt, incl HTML & Jscript: native UI dvlpmnt in C or C++, using GTK & at least one other toolkit; design & implement of Linux oper syst, incl boot & initialization, hotplug & driver load & inter-process commun usage & dvlpmnt of key oper sys components, contribution to Open Source proj used by Chrome OS, specifically the Linux kernel, GTK+/GLib, udev, DeviceKit, D-Bus, 7 Upstart, algorithms, & multithread

#1615.4815, oo prog in Java or C++: relational databases, dvlpmnt on Linux or Mac pltfrms; client-svr dvlpmnt & bldng of web svcs: dvlpmnt of web appl w/ HTML, Jscript, & CSS, & sw lifecycle for consumer-facing appl

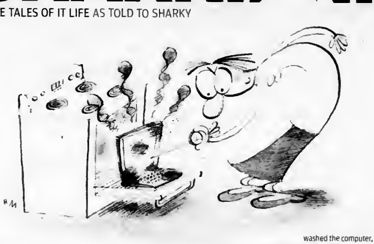
#1615.463, C++ & STL, design adv algorithms: data struct, tech research & web tech, incl HTML, CSS & Jscript

#1615.4748, frontend tech, incl HTML, CSS: Jscript, & client-srvr arch, code prog lang, incl C++ & Java, & design & dvlpmnt of high-perf, large-scale sryr appl & sw

#1615.2740: Java, Unix &/or Unix variants, script lang, databases &/or database oriented syst, & version control syst.

SHARKTANK

TRUE TALES OF IT LIFE AS TOLD TO SHARKY



Mmm! Baked Apple!

This big ad agency leases MacBook Pros for its freelancers, reports a pilot fish at the outfit that provides the laptops. "One freelancer stopped working for the company, but did not return the MacBook Pro," fish says. "Company eventually noticed they were still paying rent on this unit and worked out where it was. They requested its return and asked us to arrange collection. Meanwhile, the freelancer had fallen out with his partner, who decided to teach him a lesson by cooking the laptop. Literally. Complete with battery. What we eventually collected was not a pretty sight. We're not sure at what temperature you neeu to bake a MacBook Pro without exploding the battery and sending you and your kitchen into orbit, but this person certainly succeeded. Amazingly, the unit still worked, though the screen was damaged."

We Recommend a Low-Salt Diet

Flash back to Sri Lanka in 1980, when this pilot fish is selling early Radio Shack desktop computers to the locals, including the government's fisheries department, which uses the computer for statistical analysis. One day the agency calls to complain that the computer isn't working. Fish: How long has it been since it stopped working? Fisheries: "Uh, about a month." Fish: A month? Why didn't you call us earlier? Fisheries: "Well, it worked last month. We only use it once a month." Fish and his cohorts collect the computer, open the case – and find a layer of salt. "We have a beach hut where we keep it to stop curious employees from fiddling with it in our office," bureaucrat explains. "Of course the hut gets splashed by the waves, but the computer worked fine. Until now." Sighs fish, "So we washed the computer, motherboard and all, in soapy water. Then we rinsed it with alcohol and replaced all the CMOS, and it worked fine. And then we told the customer to please put it back in the nice air-conditioned office where we had originally installed it."

Recipe for Disaster

It's the late 1990s, and this pilot fish is working as a consultant to a big staffing firm. "The company moved into a newly vacated office building owned by a large computer manufacturer," fish reports. "All of the basement was equipped with raised flooring except for one small room. Where did the executives decide to put the minicomputer? That's right: In the one room without raised flooring. To make matters worse, that room was located immediately below the cafeteria. When the water pipes burst in the cafeteria, the mini went down in an impressive display of fireworks!"

» Feed the Shark! Send your true tale of IT life to me at sharky@computerworld.com. You'll score a sharp Shark shirt if I use it.

CHECK OUT Sharky's blog, browse the Sharkives and sign up for home delivery at **computerworld.com/sharky**.

ADVERTISERS INDEX

This index is provided as an additional service. The publisher does not assume any liability for errors or omissions.

1&1 Internet	21
APC by Schneider Electric	11
Brocade	2
Canon	17
dtSearch	35
Hewlett-Packard	C2-1
IBM Non-Intel	9
IBM Intel	C4
InterSystems	5
IT WatchDogs	35
Microsoft	33
NTT Data	15
Samsung	13, C3
SonicWALL	27
VMWare	7

BPA WORLDWIDE Periodical postage paid at Framingham, Mass., and other mailing offices. Posted under Canadian International Publication agreement PM40063731. **CANADIAN POSTMASTER:** Please return undeliverable copy to PO Box 1632, Windsor, Ontario N9A 7C9. Computerworld (ISSN 0010-4841) is published twice monthly except for the month of July by Computerworld Inc., 492 Old Connecticut Path, Box 9171, Framingham, Mass. 01701-9171. Copyright 2011 by Computerworld Inc. All rights reserved. Computerworld can be purchased on microfilm and microfiche through University Microfilms Inc., 300 N. Zeeb Road Ann Arbor, Mich. 48106. Computerworld is indexed. Back issues, if available, may be purchased from the circulation department. Photocopy rights: permission to photocopy for internal or personal use is granted by Computerworld Inc. for libraries and other users registered with the Copyright Clearance Center (CCC), provided that the base fee of $3 per copy of the article, plus 50 cents per page, is paid directly to Copyright Clearance Center, 27 Congress St., Salem, Mass. 01970. Reprints (minimum 500 copies) and permission to reprint may be purchased from The YGS Group, (800) 290-5460, Ext. 100. Email: computerworld@theygsgroup.com. Requests for missing issues will be honored only if received within 60 days of issue date. Subscription rates: $5 per copy. Annual subscription rates: – $129; Canada – $129; Central & So. America – $250; Europe – $295; all other countries – $295. digital subscription – $29. Subscriptions call toll-free (888) 559-7327. **POSTMASTER:** Send Form 3579 (Change of Address) to Computerworld, PO Box 3500, Northbrook, Ill. 60065-3500.

HAL MAYFORTH

OPINION

PAUL GLEN

Rogue IT, and Power as An Obstacle to Influence

We have to decide: Do we want to be powerful or influential?

AFTER I WROTE last month's column on why CIOs don't have more influence with "the business," I participated in a fascinating conversation with a group of big-company IT operations directors that perfectly illustrated how we in IT undermine our own influence.

The discussion turned to rogue IT, with a general consensus that it was pervasive. One estimate, which was not greatly scoffed at, was that rogue IT might constitute 15% of the average large company's IT spending.

But while nearly all of the IT leaders agreed that rogue IT was widespread, they showed little interest in exploring why that was. They didn't want to talk about what might drive line-of-business managers to bypass the IT department. They didn't want to try to understand what the experience of their business partners might be like. They weren't interested in examining whether those partners felt a lack of control, a mistrust of the department or the need for speed. By staying silent on these topics, the group seemed to be dismissing the experiences of business managers as irrelevant excuses for bad behavior.

It was another story when they were asked how to manage the situation. Silent no more, nearly everyone was suddenly spilling over with advice like this:

- **Threaten the vendors.** If vendors take meetings with the line-of-business executives without inviting IT, they should get blacklisted.
- **Require IT sign-off on purchases.** Tell the purchasing department to divert any technology-related requests to IT.
- **Refuse to integrate.** Insist on IT taking control of any systems, data and/or people that need to work with IT-controlled systems.

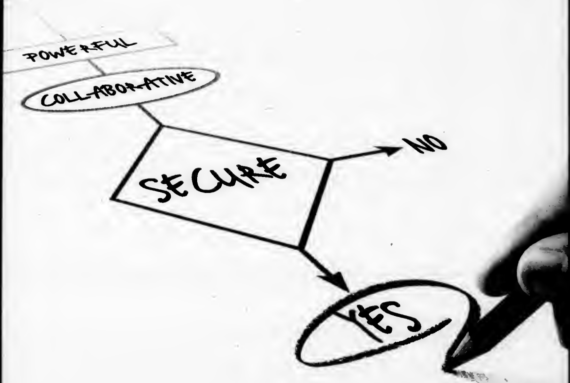
Of course, IT departments have good reasons for wanting to centralize the control of technology assets; among other things, they want to control costs and ensure that data is kept secure and managed responsibly. But notice the theme in the suggested responses to rogue IT: They all involve exercising coercive power and preventing business managers from doing what they want to do. If these IT managers had been willing to examine the experience of their business partners, they might have realized that while these techniques might control rogue behavior in the short run, the long-term effect will likely be quite the opposite.

These sorts of power moves do nothing to reduce the demand for rogue IT or to address the root causes, which often stem from negative assumptions about the experience of working with the IT department. If anything, they reinforce the beliefs that inspire business managers to go rogue and strengthen their determination to do so, ultimately driving rogue IT further underground.

Controlling attitudes and heavy-handed policies will likely undermine the efforts of CIOs who want to increase IT's influence within the business. No matter how good their personal relationships in the C-suite, their efforts to become influential will be doomed if IT is seen as an obstacle rather than a helper at every level below.

Power is about changing other people's behavior; influence is about changing other people's minds. For IT to become more influential, we must learn to examine, with empathy, the thoughts and experiences of those we want to influence. And then we will have to decide whether we want to be powerful or influential. Ultimately, we need to ask ourselves, "Are we willing to put in the effort it will take to change people's minds?" ◆

Paul Glen, CEO of Leading Geeks, is devoted to clarifying the murky world of human emotion for people who gravitate toward concrete thinking. His newest book is *8 Steps to Restoring Client Trust: A Professional's Guide to Managing Client Conflict*. You can contact him at info@leadinggeeks.com.


POWERFUL
COLLABORATIVE
SECURE
NO
YES

Because no two businesses are the same.
Introducing the flexible new range of IBM System x servers.

No two companies have the same IT requirements. That's why IBM® has a new range of System x® servers, built to handle workloads ranging from simple tasks to complex cloud-based and business applications. Featuring the latest Intel® Xeon® E5-2600 and E5-2400 series processors, these servers can be customized so that you can select features you need today and add more as your business needs change. Additionally, IBM Business Partners can help you find the server that meets your needs and pair it with the right IBM storage, networking and software solutions for a truly optimized infrastructure.

IBM System x3650 M4 Express

$3,179

OR $84 MONTH FOR 36 MONTHS

PN 7915-EBU

Low TCO with exceptional performance per watt

Flexible, "pay-as-you-grow" design to lower cost and manage risk

Excellent reliability and uptime for business-critical applications and the cloud

IBM System x3530 M4 Express

$1,899

OR $51 MONTH FOR 36 MONTHS

PN 7915-EBU

2-socket value server optimized for performance and value

Dense 1U design for many general business workloads

IBM DNA throughout including RAS flexibility and easy management

IBM System Storage® DS3500 Express

$5,499

OR $135 MONTH FOR 36 MONTHS

PN 1746A2S

6 Gbps SAS system delivers midrange performance and scalability, at entry-level prices

Up to 192 drives, high performance and nearline SAS, SSD and SED SAS drives

Four interface options: 6 Gbps SAS, 1 Gbps & 10 Gbps iSCSI/SAS and 8 Gbps FC/SAS

The new IBM System x Selection Tool can help you choose the right server and save money.
Visit:

Scan with your smart phone to learn more about the System x range

Contact the IBM Concierge to help you connect to the right IBM Business Partner.

intel inside Xeon

IBM Global Financing offerings are provided through IBM Credit LLC in the United States and other IBM subsidiaries and divisions worldwide to qualified commercial and government customers. Monthly payments provided are for planning purposes only and may vary based on your credit and other factors. Lease offer provided is based on an FMV lease of 36 monthly payments, please contact your IBM Global Financing representative for actual monthly amounts. Other restrictions may apply. Rates and offerings are subject to change, extension or withdrawal without notice. IBM hardware products are manufactured from new parts or new and serviceable used parts. Regardless, our warranty terms apply. For a copy of applicable product warranties visit http://www.ibm.com/servers/support/machine_warranties. IBM makes no representation or warranty regarding third-party products or services. IBM, the IBM logo, System Storage and System x are registered trademarks of International Business Machines Corporation, registered in many jurisdictions worldwide. Other product and service names might be trademarks of IBM or other companies. For a current list of IBM trademarks, see www.ibm.com/legal/copytrade.shtml. Intel, the Intel logo, Xeon and Xeon Inside are trademarks of Intel Corporation in the United States and other countries. All prices and savings estimates are subject to change without notice, may vary according to configuration, are based upon IBM's estimated retail selling prices as of 7/2/12 and may not include storage, hard drive, operating system or other features. Reseller prices and savings to end users may vary. Products are subject to availability. This document was developed for offerings in the United States. IBM may not offer the products, features or services discussed in this document in other countries. Contact your IBM representative or IBM Business Partner for the most current pricing in your geographic area.